(4)

To Repair or To Rebuild?

Analyzing Personnel Security Research Agendas

Carl H. Builder, Victor G. Jackson, Rae Starr

RAND | NATIONAL DEFENSE RESEARCH INSTITUTE

The research described in this report was sponsored by the Office of the Under Secretary of Defense for Policy under a Federally Funded Research and Development Center relationship with the Office of the Secretary of Defense, Contract No. MDA903-85-C-0030.

ISBN: 0-8330-0916-8

Published by The RAND Corporation
1700 Main Street, P.O. Box 2138, Santa Monica, CA 90406-2138

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER R-3652-USDP	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) To Repair or To Rebuild? Analyzing Personnel Security Research Agendas		5. TYPE OF REPORT & PERIOD COVERED Interim 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Carl H. Builder Victor G. Jackson Rae Starr		8. CONTRACT OR GRANT NUMBER(s) MDA903-85-C-0030
9. PERFORMING ORGANIZATION NAME AND ADDRESS The RAND Corporation 1700 Main Street Santa Monica, CA 90406		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS Under Secretary of Defense for Policy Washington, D. C. 20301		12. REPORT DATE September 1988 13. NUMBER OF PAGES 84
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) Unclassified 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public Release: Distribution unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

No Restrictions

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Department of Defense
Security
Espionage

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

See reverse side

DD FORM 1 JAN 73 1473

SECURITY CLASSIFICATION OF THIS PAGE When Data Entered

This report presents an evaluation of the initial research agenda of the Defense Personnel Security Research and Education Center (PERSEREC), with a proposal for new research on the personnel security problem and objectives and strategy for the Department of Defense (DOD) Personnel Security Program. The new research is proposed because the policy foundations of the current DOD program appear deficient and the current PERSEREC research agenda, which focuses primarily on detailed procedures, is unlikely to provide the basis for significant program improvements. The analysis of the current agendas reached conclusions about their completeness and priorities by inferences drawn from the agendas themselves. The proposed agenda of new research was derived from a systems-analytic or "top-down" approach. Data sources included both Executive Branch and Congressional documents; histories, descriptions, and analyses of various aspects of personnel security and espionage; and discussions with persons responsible for or experienced in personnel security matters. (ER)

R-3652-USDP

To Repair or To Rebuild?

Analyzing Personnel Security Research Agendas

Carl H. Builder, Victor G. Jackson, Rae Starr

September 1988

Prepared for the
Office of the Under Secretary of Defense
for Policy

RAND

PREFACE

Recent concern with the effectiveness of the personnel security program of the U.S. Department of Defense has led to the development of new research agendas to improve the program. This report presents an analysis of the research agendas currently being conducted and sponsored by the Defense Personnel Security Research and Education Center (PERSEREC) and assesses their completeness and the consistency of their priorities, insofar as they can be inferred from the agendas themselves. Completely new agendas for research on the foundations of the DoD personnel security program are then proposed; these proposed agendas address the nature of the personnel security problem, the objectives of the DoD program, and the strategy selected to achieve those objectives.

The report should be of interest to individuals in the Office of the Under Secretary of Defense for Policy who have responsibilities for personnel security policy and to members of the PERSEREC staff who are conducting and supporting research in this area.

This study was requested by the Under Secretary of Defense for Policy and was carried out within the International Security and Defense Policy Program of RAND's National Defense Research Institute, a Federally Funded Research and Development Center supported by the Office of the Secretary of Defense.

SUMMARY

In the wake of several significant espionage incidents involving past and present members of the Department of Defense (DoD), the Secretary of Defense in 1985 established the Stilwell Commission to review DoD security policies and procedures. Among the commission's many recommendations was the funding and instituting of security research. That recommendation led to the creation of the Personnel Security Research and Education Center (PERSEREC) at Monterey, California, and the development of research agendas to support the DoD personnel security program.

The DoD personnel security research agendas consisted of 53 research tasks in three priority categories. The first nine of those tasks were further developed or elaborated through a set of 176 research questions.

The RAND analysis of the DoD personnel security research agendas began with three objectives: (1) to assess the agendas for completeness of content and consistency of priorities; (2) to relate the agendas to the personnel security problem and to the DoD program objectives; (3) and to provide a conceptual framework for personnel security policymaking.

INITIAL REVIEW OF THE RESEARCH AGENDAS

An initial review of the research agendas revealed that they focused almost exclusively on the detailed procedures of the DoD personnel security program, as distinct from the intellective and policy foundations of the program itself. That is, very little research was to focus on the nature of the personnel security problem or on broader aspects of the DoD program. Our first conclusion, therefore, was that the research agendas appeared incomplete, whether judged by the call of the Stilwell Commission for research on both policy *and* practice or by consideration of all the elements and aspects that constitute the personnel security problem and the system necessary to deal with it.

However, that conclusion had to be tempered by the possibility that no additional research on the intellective and policy foundations of the personnel security program was needed because the nature of the problem was thoroughly understood and the program's objectives and strategy were appropriately set. Thus, to assess the completeness of the research agendas, we had to explore the state of understanding about

the personnel security problem and the extent of agreement about personnel security program policies.

THE FOUNDATIONS OF THE DoD PERSONNEL SECURITY PROGRAM

Neither literature searches nor discussions with experienced personnel security officials could provide comprehensive descriptions of the nature of the personnel security problem or clear statements of the objectives and strategy of the DoD program. The Office of the Under Secretary of Defense (Policy) publishes a comprehensive DoD personnel security program description, which was updated early in 1987, but this description covers procedures rather than policy or its relationship to the personnel security problem.

Some personnel security officials believe that the absence of comprehensive descriptions of program foundations is neither a cause for concern nor evidence of a need for research. Despite the lack of documentation, according to this view, the current program is well grounded in experience and appropriate to the problem, and research to improve its procedures is what is needed most at this time.

The conclusion we reached is quite different. We found:

- No definition of the personnel security problem—or even its boundaries with respect to other security disciplines—that would stand up under critical examination.
- No estimates of the costs, direct or indirect, for either the problem or the program that has evolved to address the problem.
- No goals between broad generalities and specific procedures.
- No basis for priorities or for tradeoffs, internal or external to the program.
- No *explicit* concepts or theories of cause and effect for the loss of secrets or damage to national security that could be tested or validated.

Moreover, these observations were supported by a number of people who are interested observers or participants in personnel security activities.

In consultation with the Office of the Under Secretary of Defense for Policy, therefore, we recast our study and divided it into two tasks: An assessment of the current research agendas within their own implied frame of reference, without independent references to the personnel security problem or program; and the development of separate, additional research agendas on the nature of the personnel security

problem and on the objectives and strategy of the DoD personnel security program.

THE CURRENT RESEARCH AGENDAS

In the absence of clearly established touchstones describing the nature of the personnel security problem and the objectives and strategy of the DoD personnel security program, our analysis was deliberately limited to logical inferences based solely on the content, focus, and balance of the agendas themselves. We found that the agendas emphasized:

- Means more than ends.
- Existing more than alternative possible means.
- Designing more than evaluating procedures.
- Details more than guiding principles.
- Procedural improvements more than problem understanding.

The logical major omissions in the current research agendas included:

- The costs of the personnel security problem or program.
- The tradeoffs between procedures, operations, and activities.
- The alternatives to current procedures, operations, activities, or theories.

ADDITIONAL RESEARCH AGENDAS

The additional research agendas we propose address (1) the nature of the personnel security problem, (2) the objectives of the DoD personnel security program, and (3) the strategy of the DoD program to meet those objectives. Establishing the need for research in these areas is probably more important at present than the details of the proposed agendas.

Two aspects of the personnel security problem warrant particular attention: the *boundary* of the problem and its *content*.

Surprisingly, *personnel security* is not formally defined. Thus, there is no way to determine the boundary between the personnel security discipline and the several other security disciplines—such as physical security and counterintelligence—that are all concerned with "keeping the nation's secrets," nor is there a clear approach to a systematic exploration of their interaction and complementarities. Also, there are

aspects of the problem of "losing the nation's secrets" that appear to be neglected because they fall "between two stools."

In the DoD program, the personnel security problem and the personnel suitability problem are essentially treated as a single problem, even though each has characteristics and implications that get slighted in the process of combination. Even if the boundaries of the personnel security problem can be more sharply drawn, the informational content within those boundaries needs to be much more coherent and accessible than it is at present. Information about the problem is almost entirely anecdotal or in the form of case histories that are unsuitable for statistical inferences. Theories about the information to be protected, human behavior, the processes that can lead to the loss of secrets, and the value of the secrets are limited, implicit, and mostly unvalidated. In the absence of comprehensive descriptions of the separate and distinguishable elements of the personnel security problem—such as deliberate compromise of classified information, security violations, and, for some, personnel suitability—there is a significant risk that remedial programs will overlook relevant information that allegedly "everyone knows." A database of descriptive information that is implicit, fragmentary, and scattered provides a poor foundation for either individual remedial measures or systematic analysis and development of theories that can provide additional insight into the nature of the problem and possible solutions.

A good description of the problem is essential because it provides the basis for the development of pertinent and achievable objectives. The current practice of treating the personnel security and personnel suitability problems together has constrained the operative objective of the DoD personnel security program to the "least common denominator" applicable to both problems. Thus, the objective of seeking to "accept and retain personnel . . . and deny, grant and revoke clearances . . . consistent with the interests of national security" arbitrarily, unnecessarily, and adversely limits the scope of programs whose true objective has something to do with keeping the nation's secrets.

If, as we believe, the current statements of the personnel security problem and the objectives of the DoD program are deficient, it is not surprising that questions can be raised about the adequacy of the DoD strategy. The heavy emphasis on preclearance investigations does not seem appropriate, given the fact that many spies became disloyal after receiving a clearance. Similarly, periodic reinvestigations do nothing to staunch the compromise of classified information in the interval between investigations.

One senior official responsible for personnel security policy compared the personnel security program to a leaky bucket that gets a new

patch with every new espionage case. The patches weren't the best solution, but he couldn't do away with them until he had a new and tested bucket. The current research agendas appear to be oriented toward newer and better patches. Here, we argue for additional research agendas to design and test a new bucket.

ACKNOWLEDGMENTS

The authors wish to thank William R. Fedor, the Deputy Director of Counterintelligence and Investigative Programs in the Office of the Under Secretary of Defense for Policy, for his support and cooperation in the conduct of this research; Carson K. Eoyang, the Director of the Defense Personnel Security Research and Education Center, for information and discussions of his program of personnel security research; RAND colleagues Glenn A. Gotz and Richard J. Kaplan for helpful comments on an early draft of this report; and RAND colleague Janet M. DeLand for extensive editorial assistance.

CONTENTS

FIGURES

TABLES

ACRONYMS

CIA	Central Intelligence Agency
COMSEC	Communications Security
DIA	Defense Intelligence Agency
DIS	Defense Investigative Service
DISCO	Defense Investigative Service Clearance Office
DMDC	Defense Manpower Data Center
DoD	Department of Defense
DoE	Department of Energy
DUSD(P)	Deputy Under Secretary of Defense (Policy)
FBI	Federal Bureau of Investigation
GRU	Chief Intelligence Directorate of the Soviet General Staff
IBI	Interview-Oriented Background Investigation
IRS	Internal Revenue Service
JCS	Joint Chiefs of Staff
KGB	Committee for State Security of the Soviet Union
MEPS	Military Entrance Processing Stations
NPS	Naval Postgraduate School
OPM	Office of Personnel Management
OSD	Office of the Secretary of Defense
PERSEREC	Personnel Security Research and Education Center
PIC	Personnel Investigation Center
PR	Periodic Reinvestigation
PRP	Personnel Reliability Program
PSP	Personnel Security Program
SBI	Special Background Investigation
USA	U.S. Army

I. INTRODUCTION

BACKGROUND

> The importance of espionage in military affairs has been recognized since the beginning of recorded history. The Egyptians had a well-developed secret service, and spying and subversion are mentioned in the *Iliad* and in the Bible. Sun Tzu's treatise (c. 500 B.C.) on the art of war in China devotes a chapter to espionage. In the middle ages political espionage became important. Joan of Arc was betrayed by Bishop Pierre Cauchon of Beauvais, a spy in the pay of the English, and Sir Francis Walsingham developed an efficient spy system for Elizabeth I. With the growth of the modern national state, systemized intelligence became a fundamental part of government in most countries.[1]

Spies and spying have a long and, popularly judged, unsavory history.[2] Spying against the United States in the post-World War II period has presented a mixed picture: The years 1973–1975 have been described as a "watershed . . . a period of relative calm prior to the escalating frequency of [espionage] events in the late 70s and the present decade."[3] The amount of damage done to the United States by this recent spying is somewhat uncertain, because we do not know exactly how many and which secrets were betrayed, but enough is known to support a widespread belief that the damage has been massive.[4]

---

[1]*The New Columbia Encyclopedia*, Columbia University Press, New York, 1975, pp. 891–892.

[2]In Michael J. Barrett's pithy comment, "Espionage is the world's second oldest profession and just as honorable as the first." Quoted by Phillip Knightly in *The Second Oldest Profession*, W. W. Norton & Co., New York, 1986, Frontispiece.

[3]*Recent Espionage Cases*, U.S. Department of Defense, Defense Security Institute, January 1987, p. 1.

[4]Considering only the peacetime consequences of the Walker-Whitworth case alone, Rear Admiral William O. Studeman, the Director of Naval Intelligence, testified that recovery from these espionage activities will take many years and millions of dollars (*Meeting the Espionage Challenge: A Review of United States Counterintelligence and Security Programs*, Report of the Select Committee on Intelligence, United States Senate, 99th Congress, 2d Session, Report 99-522, p. 102). Regarding the possible wartime consequences of this same case, Soviet KGB defector Vitaly Yurchenko asserted that he was told by a high KGB official that the information learned from the Walker-Whitworth operation would have been "devastating" to the United States in time of war (*Meeting the Espionage Challenge*, p. 104). Secretary of the Navy John F. Lehman, Jr. was even more explicit: "Had we been engaged in any conflict with the Soviets, it could have had the devastating consequences that Ultra [the code name for the intelligence resulting from broken German ciphers in World War II] had for the Germans." (John Barron, *Breaking the Ring*, Houghton Mifflin Co., Boston, 1987, p. 212.)

In reaction to this problem, Secretary of Defense Caspar W. Weinberger on June 25, 1985, appointed a commission headed by General Richard G. Stilwell, USA (Ret.), to review and evaluate Department of Defense (DoD) security policies and procedures. This commission completed its work and submitted its report on November 19, 1985.[5]

The Stilwell Commission report focuses on the protection of classified information—as distinct from unclassified but sensitive information—and contains three major substantive sections. These are: Policy and Procedures, Management and Execution, and Resource Impact. The report makes 63 specific recommendations, most of which concern policy and procedures. One of the recommendations was that research should be funded to support security policies and procedures. The commission tended to emphasize research on personnel security but also included research on information security and physical security.[6]

The most important consequence of the recommendation to fund and institute research was the creation by the DoD of the Defense Personnel Security Research and Education Center (PERSEREC) and the assignment to it of a range of functions relevant to personnel security research and education. PERSEREC is a tenant organization of the Naval Postgraduate School (NPS), Monterey, California, and reports to the Superintendent of the NPS. Policy guidance for PERSEREC is provided by the Deputy Under Secretary of Defense for Policy.[7]

PERSEREC is currently conducting and supporting research on personnel security, pursuing the first 10 of 53 research tasks identified by DoD and PERSEREC in mid-1986. Each of these research tasks is assigned one of three priority categories, reflecting the judgments of experienced security personnel about their urgency.

These research agendas are the result of a "bottom-up" approach that begins with current concerns about operational programs and procedures. This approach ensures that the identified research tasks are directed toward "real world" problems as seen by persons with responsibilities in the area and that "real world" operators will apply the research results. However, we believe that it poses several risks:

---

[5]*Keeping the Nation's Secrets: A Report to the Secretary of Defense by the Commission to Review DoD Security Policies and Practices*, Office of the Secretary of Defense, November 19, 1985.

[6]*Information security* includes the creation and control of classified information; *physical security* includes physical measures to prevent unauthorized access and safeguard against espionage; and *personnel security* includes measures relevant to persons who will be trusted with access to classified information. These definitions are discussed more fully below.

[7]Department of Defense Directive No. 5210.79, Subject: Defense Personnel Security and Education Center (PERSEREC), February 19, 1986.

- The research agendas may not be complete because of simple oversights or limitations in operator experience, or because the tasks have been confined to current procedures and perceptions of the problems.
- The rationale for the priorities in the agendas may not be definable, explainable, or supportable.
- The operational programs, procedures, and concepts that are the starting point for the research may be the result of a process of evolution in which the rationale and effectiveness of the system are no longer entirely evident.
- The 53 research tasks and three priority categories may not, by themselves, provide an overall, integrated conception of the personnel security problems, policies, and procedures that will guide subsequent modifications of the agendas and priorities as the research program develops.

PURPOSE AND SCOPE OF THIS ANALYSIS

The RAND analysis was undertaken to provide an independent assessment of the research agendas and their relationship to the personnel security problem and program. Its specific objectives were:

1. To ensure that the current research agendas are demonstrably complete and logically ordered in priority.
2. To relate these research agendas to the personnel security problem (or problems) and to the program objectives.
3. To provide conceptual frameworks for personnel security policymaking.

Instead of taking a "bottom-up" approach, the RAND study team deliberately chose a "top-down" approach structured to ensure systematic coverage of a hierarchy of elements that begins with the problem to be solved and leads through logically related steps to the ultimate solution. This systems-analytic approach is particularly useful for examining very large and complex problems, programs, and their interrelationships.

Our original analytical objectives were not achievable because several essential prerequisites are missing. An assessment of the appropriateness of operational programs (or of the research to support such programs) depends upon clear definitions of the motivating problem(s), the objectives or goals of the program, and the strategy that guides the allocation of resources to achieve those objectives. While we were prepared to clarify, refine, or elaborate upon existing

definitions of such fundamental elements, we did not have the basic information necessary to create them from scratch. For the personnel security problem and program, these essential definitions are either missing or of questionable relevance or suitability and will require significant research to develop.

Our analysis was therefore reoriented toward two new objectives:

1. Evaluating the current PERSEREC research agenda for completeness in content and consistency in priorities, insofar as these assessments could be inferred from the agendas themselves.
2. Developing additional agendas of research on the personnel security problem, selecting objectives for the personnel security system, and selecting a strategy to guide the allocation of resources to achieve those objectives.

ORGANIZATION OF THE REPORT

Section II describes our understanding and assessment of the DoD personnel security problem and program. It summarizes our perspective of the situation that confronts policymakers who must deal with the personnel security problem. Sections III and IV present the substantive results of our analysis. The current research agendas are analyzed on the basis of their own content in Sec. III, and Sec. IV describes our proposed additional agendas for new research. Section V summarizes our conclusions and observations. Appendix A contains the current research agendas; App. B is a glossary of relevant terms; and App. C extends the analysis of Sec. III by providing the details of a topic-by-topic examination of the current research agendas.

II. PERSONNEL SECURITY

This section outlines our general appreciation of the current DoD personnel security problem and program. It is based on information in the literature and discussions with people involved in, or concerned with, personnel security issues.

THE PERSONNEL SECURITY PROBLEM

The personnel security problem consists basically of people who have been entrusted with matters affecting institutional well-being violating that trust and behaving in ways that adversely affect the institution. This formulation of the problem applies equally well to the federal government, the DoD, other agencies, or even a commercial enterprise.

The DoD personnel security problem could be perceived as DoD personnel who have violated their trust with matters affecting national security. Few would disagree with that perception, but there are other possible perceptions, depending on the interpretation of *which* matters affect national security.

Some would define matters affecting national security as the loss of the nation's secrets through espionage; others would narrow the definition to Communist or Soviet spying. Others would broaden the definition to include the behavior of cleared personnel with respect to such things as alcohol, drugs, finances, and sex. This range of interpretations allows for considerable latitude in perceptions of the problem and solutions.

While the much publicized spy cases, such as the recent Walker-Whitworth case, are generally perceived as the most serious manifestations of the DoD personnel security problem, "leaks" and violations of security procedures are also considered by many to be a serious part of that problem.

While loss of the nation's secrets is generally considered to be the major personnel security problem, the problem also includes human reliability in positions of trust that have little or nothing to do with the loss of secrets, but much to do with the security of valuable people and sensitive property such as nuclear weapons. Thus, the problem ranges from losing the nation's secrets to accepting the "wrong" people for important or sensitive jobs.

The narrower the definition of the personnel security problem, the more the number of omitted elements that some will argue should or must be included. The broader the definition, the more difficult it becomes to separate personnel security problems from problems traditionally associated with personnel management, or to prevent them from lapping over into other security areas, such as counterespionage or physical security. This lack of sharp definition leads to a number of difficulties:

- It leads to misaligned disputes about solutions.
- It diffuses efforts to solve the problem in its manifold forms.
- It encourages a focus on means rather than ends because the former become more apparent than the latter.
- It allows priorities to be set by the available means rather than the nature or character of the problem.
- It permits the problem to "drift" across bureaucratic domains, with risks of overlapping or conflicting responsibilities or of gaps in problem coverage.

The explicit definition of the personnel security problem is likely to remain a contentious issue. The people with a stake in the definition—and the eventual solution—of the problem include:

- The defense policymakers, who are ultimately held responsible for the keeping of the nation's security.
- The defense contractors, who generally find security procedures to be a burden of dubious value and a hindrance in the employment of critical people and skills.
- The personnel security professionals, particularly those in investigative and personnel management fields, whose careers have been established in the prevailing perceptions of the problem and its solution.
- The military commanders and government officials who are responsible for implementing personnel security procedures and who are accountable in any security breaches.
- The civil libertarians who are concerned about the preservation of individual rights and freedoms under any personnel security program.
- Security professionals in adjacent areas such as counterintelligence or physical security, where an expanded definition of the personnel security problem might denigrate or encroach upon their efforts.

While those who are responsible for personnel security may reasonably hope that technology and adequate funding will aid them in the future, the adverse trends are all too apparent:

- Information is burgeoning in importance and extent for national security. Possession of, access to, management of, and communication of information have become central to most modern weapon systems. The only secrets on a battlefield were once maps and messages, but even the circuit boards or microchips in a projectile may be secret today. Whatever steps may be taken to reduce the amount of classified *documents*, the historical trend is to rely more and more on the secrecy of information for national security.
- Technology, particularly computer technology, is making the transfer and, therefore, the theft of massive amounts of information easier.
- Trends in societal attitudes within the United States and elsewhere favor more individual freedom and rights, less government secrecy, and more litigation—all of which make what appear to be discriminative and intrusive approaches to personnel security more difficult.
- Societal attitudes toward governments, the military, and the observance of proscriptive laws appear to be changing adversely; in the most recent espionage cases, motivations appear to be shifting from ideology to avarice.

The personnel security problem has been changing and probably will continue to change over time. Moreover, the conditions and debates about solutions look as though they are getting worse, not better, unless research brings new understanding to bear.

THE DoD PERSONNEL SECURITY PROGRAM

The DoD personnel security program that has evolved over the past 30 years is almost entirely centered on clearances, which are granted, denied, or revoked on the basis of background investigations into employees' identities, associations, and behavior.[1] Clearance permits indefinite access to classified information or assignment to sensitive positions, subject only to:

---

[1]The program is described in *Personnel Security Program*, Department of Defense, Office of the Deputy Under Secretary of Defense (Policy), DoD 5200.2-R, January 1987.

- The highest security level authorized for access by the clearance, generally reflecting the extent of the background investigation.
- The local commander's or supervisor's judgment of a need-to-know for access to information or suitability for the assignment.
- Subsequent behavior or associations that call the person's suitability for a clearance into question.
- Termination of employment or duty.
- Periodic reinvestigation of associations and behavior.

By any measure—the allocation of people and funding or the focus of policies and research—the DoD personnel security program has been based almost entirely on background investigations for the granting of clearances. On-the-job monitoring and education have been relatively minor efforts by comparison. Other than "debriefings," the program has no provisions for personnel whose clearances have ended.

Several recent, highly publicized spy cases have brought the security programs of all government agencies under scrutiny: Where and why did the existing programs fail? The Stilwell Commission found that the DoD security program had been "reasonably effective" but made a number of recommendations for improvement:

- Reductions in the number of clearances.[2]
- Improvements in the quality of the investigation and adjudication processes.
- Reductions in the backlog of periodic reinvestigations for people holding clearances.[3]
- Greater differentiation and prioritization of security efforts (i.e., investigations and adjudication criteria) according to the sensitivity of the information or position in question.
- More sanctions against those violating security rules, particularly civilians and contractors.
- Better training and education for all involved.
- Basic research to guide security policy and procedures.[4]

---

[2]This recommendation has recently been implemented; the number of active DoD clearances has been reduced from about 4 million to 2.5 million by revoking those held by personnel who had no need or only marginal need for access to classified information.

[3]Until recently, periodic reinvestigations were largely deferred in the press of investigative and adjudicative work associated with granting initial clearances. The current goals require that the holders of all outstanding clearances be reinvestigated by 1995 and at least every five years thereafter. This has resulted in a noticeable increase in the time required to grant new clearances, suggesting an imbalance between investigative requirements and capabilities.

[4]Instituted in the creation of PERSEREC.

All of these recommendations have either been implemented or are currently under consideration. Limited, experimental use of polygraph examinations has been permitted as an adjunct to background investigations. Personnel monitoring modeled after the "human reliability" programs used to protect nuclear weapons is being considered for some personnel assigned to very sensitive positions or having access to very sensitive information. Otherwise, the DoD personnel security program appears to be aimed at doing a better job of doing what it has been doing—and, with minor changes, doing it the way that it has been—mostly by investigating people to clear them for sensitive positions or access to classified information.

AN ASSESSMENT OF THE PERSONNEL SECURITY SITUATION

There is little doubt that a large-scale, diverse, and hostile intelligence effort is directed against the United States. Apparently the effort is disturbingly successful, with high peacetime costs to the United States and alarming potential wartime costs. It is generally conceded that this threat cannot be completely thwarted:

> While no system of security can provide foolproof protection, it can make espionage more difficult to undertake and more difficult to accomplish without detection; and it should minimize the compromise of classified information whatever the cause.[5]

Moreover, some societal trends suggest that the frequency and number of incidents of espionage may increase, quite apart from hostile intelligence efforts, simply because of changing attitudes and values in the American society. Despite reductions in clearances and classified documents, the amount of classified information and the nation's dependency upon it for security are likely to increase. Under these circumstances, the danger of costly failures in security will probably increase. That is a risk that the nation must face.

At the same time, however, *there may be failures in security that are more embarrassing to the security programs than they are costly to the nation's security*. Those are risks the security programs must face. To the extent that the current security programs are inefficient, ineffective, unresponsive, or irrelevant and are perceived as such, they will be criticized in publicized cases, regardless of the actual damage incurred. And the more intrusive and discriminating security programs are, the more they will be challenged. In sum, the risks the security programs

[5]*Keeping the Nation's Secrets*, p. 7.

run by being inefficient and ineffective may be rising faster than the risks to national security.

While a number of security disciplines, including personnel security, can be applied to counter the threat of espionage, no basis exists today for a systematic analysis and comparison of their relative costs, capabilities, or limitations. That requires a definition of the problem and a description of the costs and benefits of the alternatives. The Stilwell Commission concluded that such comparisons are "hampered by the lack of firm data and meaningful analysis in several aspects of the security equation."[6] Thus, there is no objective basis for deciding whether or how much additional emphasis should be placed on personnel security.

Within the DoD personnel security program itself and the research now contemplated to support it, there is no apparent consideration of alternatives to the approach of issuing clearances based upon background investigations. The heavy emphasis on such investigations appears to be the result of history and pragmatism rather than theory or deliberate choice. While background investigations may not necessarily reveal or predict future trustworthiness, they may reveal past evidence of untrustworthiness or unreliability that justifies denying an applicant a position of trust. The origins of this approach to the personnel security problem appear to lie in techniques for screening job applicants, where certain behavioral aspects are taken to be predictive of job suitability. The utility or effectiveness of this approach for personnel security programs seems not to have been questioned much, if at all, until long after it was well established in the 1950s.

The DoD personnel security program would almost certainly benefit from a fundamental redefinition and restructuring to distinguish between the issue of personnel suitability and that of "keeping the nation's secrets." There is no reasonable quarrel with the establishment of suitability criteria for government employees, whether or not they will ever have access to classified information. Whether or not suitability can be judged by such aspects as reliability, trustworthiness, and loyalty—or how these terms can be made operational—may be more debatable.

There is reason to quarrel, on the other hand, with the *combining* of suitability and security issues. The aggregation of personnel measures appropriate for "keeping the nation's secrets" both differs from and is larger than the aggregation of measures appropriate for selecting and retaining employees. Requiring that personnel who receive clearances

[6]*Keeping the Nation's Secrets*, p. 13. We take "the security equation" to mean the relationships between security and the various security efforts.

should be "reliable, trustworthy and loyal" is only one means to the end of keeping the nation's secrets. There are others that have no connection with these traits (see below).

When disparate goals are combined under a single program, those that are more easily addressed will tend to dominate the program's activities and procedures. Evidence of the dominance of personnel suitability goals in the personnel security program can be seen in the extreme imbalance between the effort to investigate people before granting them clearances and the effort to follow up on those people after their separation from employment or service. The current combination of and confusion between personnel suitability measures and personnel security measures has resulted in harmful and unnecessary constraints on the effectiveness of security measures.

It is not apparent what fraction of the problem of keeping the nation's secrets can and should be countered through the personnel security program, rather than other security measures or programs. There is simply no basis available for trading some personnel security measures off against others.

The personnel security program is vulnerable to being held accountable for embarrassing security failures that result from any number of human frailties and motivations. The program has painted itself into a corner by not exploring alternative approaches, by claiming rather than proving the validity of its current approach, by elaborating rather than questioning its procedures and thereby becoming less credible to those it serves.

Modest changes and incremental improvements to the current program are not likely to produce a significantly more effective DoD personnel security program. Major investments in improving the effectiveness or efficiency of current procedures should be deferred until the theoretical foundations of the program are thoroughly examined to provide a clearer understanding and more complete description of the personnel security problem. In the light of that understanding, a careful examination should be made of alternative objectives for the DoD personnel security program and their implications for program feasibility, effectiveness, and cost.

III. ANALYSIS OF THE CURRENT RESEARCH AGENDAS

INTRODUCTION

The Analytical Problem

The principal objective of the study reported here was to insure that the agendas for personnel security research were complete and that priorities were correct according to some explainable logic. The approach chosen, as noted earlier, was a top-down systems analysis of the personnel security system, including the personnel security problem, policies, and procedures and their relationships to each other and to surrounding systems, such as the physical and information security systems. We hoped that this analysis would enable us to build simplified models (or conceptual frameworks) of the system that could be used much more easily than the complex system itself to analyze the research agendas for completeness and priorities.

We expected to find some gaps in information about the personnel security problem and the relationships among policies, procedures, and the other surrounding systems. Such gaps are typical in any large, complex, mature system, where procedures and policies have taken on a life of their own and have become disconnected from their original roots. The problem they were devised to address may have changed over time, leaving the policies behind; or the procedures may not have kept pace with the policies. Such gaps can usually be identified and filled in through logical inferences. They would be expected to be the subjects of most of the recommended additions to complete the research agendas.

But as we gathered information about the personnel security system, we found more than gaps and minor disconnects that had to be bridged: The problem was not adequately defined or bounded to enable us to undertake a systems analysis. If we tried to infer the problem from the policy statements, it became too broad and vague; if we tried to infer it from the procedures, it became too narrow.

Defining the personnel security problem sufficiently to permit a systems analysis appeared to be a major research effort in itself. And that definition would have a major influence on key aspects of the design of policies to address the problem, which also required careful research to explore the alternatives and implications of design choices.

In view of the amount and depth of research needed just to define the personnel security problem and the program objectives and strategies, it was apparent that the additional research agendas to address these several aspects would bear little or no relationship to the current research agendas. Thus, it was necessary to create additional research agendas to address the personnel security problem and the program objectives and strategies, in addition to analyzing the current research agendas in the context of the current personnel security program.

Our analysis of the current research agendas is neither top-down nor systems-analytic. It takes a perspective that might be attributed to a stranger with a logical mind who is asked to look at these agendas to discern, if possible, whether anything might be missing or out of order. Thus, this analysis is deliberately restricted to inferences from the agendas themselves. If issues outside the current research agendas had been considered, they would have soon swamped the agendas with their numbers and relative importance. We therefore attempted to stay within the boundaries of the current agendas to speak to those who do not share our view about the more general and unresolved issues.

Current Research Agendas

The current research agendas were developed by a conference committee[1] as a proposed agenda of personnel security research to be undertaken by PERSEREC. The agendas are reproduced in App. A. They consist of 53 tasks in three priority categories. Each of these tasks is described briefly to convey the focus or purpose of the desired research. The first priority category consists of the 10 tasks that were to be pursued first by PERSEREC; the second category consists of another 10 tasks to be pursued after the first 10 have been funded and initiated; the third category consists of the remaining 33 tasks, which were considered to be less cost-effective research investments than the previous 20.

Nine of the 10 first-priority tasks were further developed or expanded in sets (or tabs) of questions. Some of the resulting 176 questions were broader than the task they were intended to define; indeed, a few appeared to exceed their parent task as a research challenge and could rival many of the 53 tasks in breadth and importance. Therefore, this analysis includes the questions as an independent set alongside the tasks.

---

[1]The conference was held on May 21–23, 1986, at the Xerox Training Center, Leesburg, Virginia.

Assumptions About the Agendas

For the purpose of this analysis, we have assumed the tasks and questions of the research agendas to be:

1. *Collectively*, a fair sampling of the character of the personnel security program and the concerns of the people responsible for it. The current research agendas are a good mirror of the problems and issues thought to be important and researchable by those involved with the personnel security program.
2. *Individually*, valid research tasks or questions. The current research agendas are composed entirely of tasks and questions that are both pertinent and researchable.

Both of these assumptions are made for analytic convenience rather than descriptive accuracy. The first assumption allows the current research agendas to define the scope of the personnel security program and its research interests.[2] In all probability, these agendas have inadvertently excluded some broader problems or issues of concern, but to search out those problems or issues would require an overall top-down analysis of the program. Such an analysis is provided in Sec. IV.

The second assumption accepts each of the tasks and questions without challenge as to their research utility or feasibility. While the tasks are clearly of varying stature on these aspects, they cannot be individually judged solely on the basis of the brief statements provided or in the absence of an analytic framework for evaluating the overall program. Thus, it is analytically convenient to assume that they are all pertinent and researchable.

We assume that the tasks and questions are the consequence of an implicit but legitimate set of perspectives. The only questions asked in this analysis are:

- Is there something obviously missing?
- What, if anything, needs to be added?
- Is there something obviously out of order?
- How should the order be arranged logically?

---

[2]This illustrates a consequence of using the current research agendas as an "outsider's window" onto the personnel security program. It suggests that the broad outlines of the program—the problem it addresses and the principal means employed to solve that problem—may be inferred from the research agendas. If the agendas were very small, such an inference would be weak, if not unfair. But with 53 research task statements and 176 high-priority research questions to work with, an outsider would be reasonably justified in assuming that he or she could learn a great deal about the program.

ANALYTIC APPROACH

Sorting the Agendas by Subject

The 53 tasks and 176 questions were sorted by the subject matter (topic or function) they addressed. The subjects or topics were suggested by the tasks and questions themselves. For each task (or question), we asked, If this task (or question) were to be put into a bin, what label would be on that bin?

Seven topics or functions emerged, as shown in Table 1, listed in order of the number of tasks associated with each. The sixth and seventh topics, *Program* and *Problem*, are the focus of only three tasks each, but they are proportionately better represented among the questions.[3] While one function, *Screening*, is not found among the questions, it is well represented among the tasks. Thus, each of the topics is sufficiently represented in the current research agendas to justify its distinction for the purposes of analysis.

Table 1

TOPICS IN THE CURRENT RESEARCH AGENDAS

Topic	Number of Tasks	Priority Category I	II	III	Number of Tab Questions
Investigation	18	4	5	9	52
Monitoring	11	3		8	29
Clearances	7		1	6	3
Screening	6		1	5	0
Adjudication	5	3		2	68
Program	3		2	1	7
Problem	3		1	2	17
Totals	53	10	10	33	176

Hierarchical Structure

These seven topics and functions were then arranged within a hierarchy according to their logical relationships to each other. Each topic or function was placed directly beneath those it would logically

[3]*Program* was listed ahead of *Problem* only because it was associated with more of the higher-priority tasks.

support, possibly in parallel with one or more others providing independent support.[4]

Constructing this hierarchy provided one of the first analytical checks for omissions in the current research agendas: Were any logical topics or functions obviously missing? Additional (implied) topics or functions could be added at this stage if necessary to connect several supporting topics and complete the hierarchy. No additional topics or functions were required to complete a logical hierarchy involving the seven topics and functions. However, *Clearances* appeared to be logically divisible between the initial *granting and denying* of new clearances and the *revoking* of existing clearances. A reexamination of the current research agendas showed that the division was justified: One of the tasks was devoted entirely to revoking existing clearances and not at all to the granting or denying of clearances.

Our functional hierarchy is shown in Fig. 1. The arrangement of the functions is intended to illustrate a logical set of relationships among them, not the flow of work or the balance of effort. For example, the screening of applicants by interview, questionnaire, or testing may precede *any* investigation. Yet some kind of investigation may (or may not) be involved in the screening of applicants. Likewise, the monitoring of behavior may (or may not) involve investigations, yet the adjudication of information is *always* based on some kind of investigation. Thus, while investigations may support screening, adjudication, and monitoring, their relationship to adjudication is different (or more certain) from that with screening and monitoring.

At each level of the hierarchy, we collected the corresponding tasks and questions of the current research agendas and analyzed them to determine the implied focus and potential scope of the current personnel security program—what was included, what might have been omitted, and where the program appeared to be focusing its interests and concerns. This analysis provided the basis for suggesting additional research tasks to cover the omissions and for setting the priorities among the tasks at *any given level.*

The priorities among tasks at *different levels* can only be implied from the levels themselves. Within the functional hierarchy developed here, each level can be interpreted as *means* for the level immediately above and as an *end* for the level immediately below. All other things being equal, defining the end completely and properly is generally a higher-priority task than defining the means to that end, since the

[4]There are formal methods for arranging hierarchies, such as the one described by Thomas L. Saaty in *The Analytic Hierarchy Process*, McGraw-Hill, New York, 1980, but neither the required effort nor the analytic sophistication was deemed appropriate here because of the analytic constraints in this study.

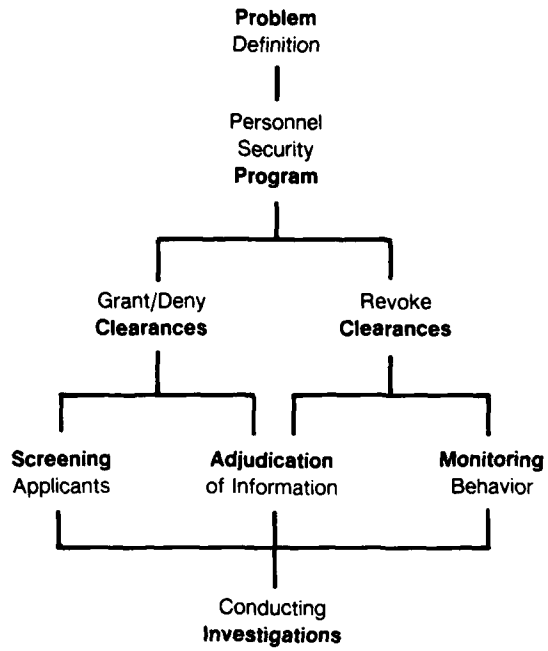

Fig. 1—Functional hierarchy of topics, as inferred from the current research agendas

soundness of the latter depends upon the validity of the former. That logic would argue for priorities according to the levels—from top to bottom—in the hierarchy. However, all other things are usually not equal: An end or problem may be sufficiently understood to make the design of means or solutions more urgent, albeit at some risk.

Thus, the setting of priorities among tasks at different levels depends on judgments about the state of knowledge, risks, problems, and the opportunities at each level. In the absence of such judgments, prudence would argue for setting the priorities according to the levels of the hierarchy; but *with* such judgments, any ordering can be justified. Orderings of priorities other than that suggested by the hierarchy necessarily implies such judgments, which can be inferred and, therefore, questioned.

OVERALL ANALYSIS OF THE AGENDAS

Analysis of the 53 Tasks

The 53 tasks of the current research agendas are distributed within the functional hierarchy shown in Fig. 2. It is apparent that the weight of the agendas falls upon the lowest two levels. Indeed, Level IV appears to be the "center of gravity," with 22 tasks at that level, 13 above it, and 18 below.[5] Perhaps most significantly, none of the 10 first-priority tasks are concerned with the top three levels of the hierarchy.[6]

Most of the urgent or important research issues appear to be associated with uncertainties or concerns about the the lowest two levels of the hierarchy—about the means more than the ends of the program. The upper three levels—the nature of the personnel security problem, the design of the overall program to address it, and the role of clearances as the principal (if not only) instrument in that program—appear to be better settled or less urgent, important, or tractable than screening, adjudication, monitoring, and investigation.

The distribution of the 53 tasks is shown in more detail in Tables 2, 3, and 4. Table 2 shows the alignment of the 10 first-priority tasks with the eight functions and five levels of the hierarchy; Table 3 shows the alignment of the 10 second-priority tasks; and Table 4 shows the alignment for the 33 third-priority tasks. These tables illustrate both the balance of the tasks across the levels of the hierarchy and the tasks that stand out as notable extremes in that balance.

Table 2 shows clearly that the 10 first-priority tasks are entirely devoted to adjudication, monitoring, and investigation. Not even screening, also at the fourth level of the hierarchy, is included among the highest-priority tasks. The emphasis on the lower levels is accentuated by comparison with the 10 second-priority tasks in Table 3, which indicates a much more balanced alignment of tasks across the five hierarchy levels. A similar observation can be made about the 33 third-priority tasks in Table 4.

From the most cursory examination of Tables 2, 3, and 4, six tasks stand out. Three of them have to do with defining the personnel security problem:

---

[5]If the 53 tasks were uniformly distributed across the eight functions of the hierarchy, the upper three levels would be twice as populated as they are, and the lowest level would be less than half as populated as it is. Level IV, the most populated level, would remain essentially as it is.

[6]However, a number of the tab questions associated with these first-priority tasks are concerned with the upper three levels of the hierarchy.

Level	Priority I	II	III	Total Tasks
I		1	2	3
II		2	1	3
III		1	6	7
IV	6	1	15	22
V	4	5	9	18
	10	10	33	53

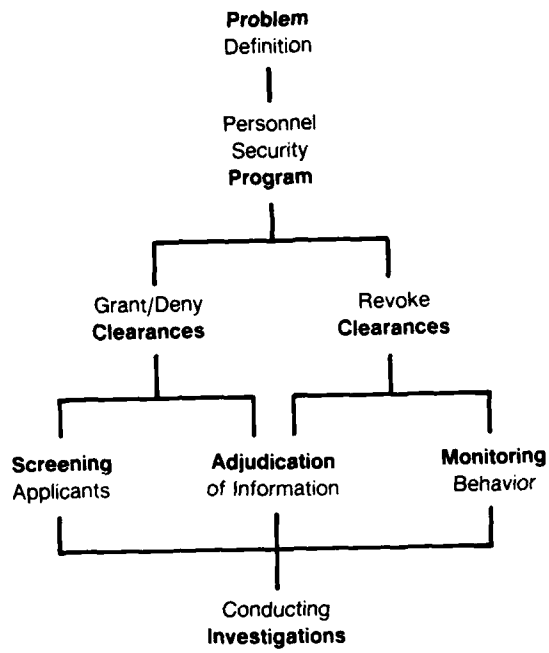

Fig. 2—Agenda tasks within the hierarchy

Table 2

ALIGNMENT OF FIRST-PRIORITY TASKS WITH HIERARCHY LEVELS

Hierarchy Level							
I	II	III		IV			V
Problem	Program	Grant/Deny Clearance	Revoke Clearance	Screening	Adjudi-cation	Monitor-ing	Investi-gation
							I-1
					I-2		
							I-3
						I-4	
						I-5	
					I-6		
					I-7		
							I-8
						I-9	
							I-10

Table 3

ALIGNMENT OF SECOND-PRIORITY TASKS WITH HIERARCHY LEVELS

Hierarchy Level							
I	II	III		IV			V
Problem	Program	Grant/Deny Clearance	Revoke Clearance	Screening	Adjudi-cation	Monitor-ing	Investi-gation
				II-1			
II-2							
							II-3
			II-4				
							II-5
							II-6
							II-7
							II-8
	II-9						
	II-10						

Table 4

ALIGNMENT OF THIRD-PRIORITY TASKS WITH HIERARCHY LEVELS

Hierarchy Level							
I	II	III		IV			V
Problem	Program	Grant/Deny Clearance	Revoke Clearance	Screening	Adjudi-cation	Monitor-ing	Investi-gation
				III-1			
				III-2			
				III-3			
				III-4			
							III-5
				III-6			
							III-7
							III-8
		III-9					
							III-10
							III-11
							III-12
							III-13
					III-14		
					III-15		
						III-16	
							III-17
						III-18	
						III-19	
		III-20					
						III-21	
						III-22	
						III-23	
						III-24	
							III-25
		III-26					
III-27							
	III28						
III-292							
						III-30	
		III-31					
		III-32					
		III-33					

1. Collect and analyze personal history and behavioral data for known espionage cases to determine if they show behavioral patterns that could have led to their early detection. [II-2][7]
2. Identify high risk/high leverage billets; develop a way of assessing security importance of billets. [III-27]
3. Review statistical literature to identify techniques that might be used in predicting personnel security risks. [III-29]

All three tasks would contribute to an understanding of the problem the personnel security program is addressing (or is supposed to address). The first (Task II-2) would gather basic data essential to understand the espionage problem and then would look for relationships that are essential to the validity of the theories that are the foundations of the current personnel security program. The other two (Tasks III-27 and III-29) would pursue basic aspects of risk in the personnel security problem.

But several aspects of the personnel security problem are not evident among these three tasks: None of the tasks address the scope or size of the problem, its costs (direct and indirect) to the nation, its relationship to (and tradeoffs with) other security problems such as physical and information security, or the character and mechanism(s)[8] the problem may exhibit in the past, present, and future. It seems unlikely that all of these absent issues are well or broadly understood; if they were, they would be much more apparent in the available literature.

The other three tasks that stand out in Tables 3 and 4 concern the personnel security program as a whole:

1. Develop a personnel security management information system. [II-9]
2. Develop a cost-benefit framework for evaluating personnel security programs and proposals. [II-10]
3. Identify means to develop in organizations a pro-security ethic compatible with traditional American values. [III-28]

---

[7]The numbers in brackets refer to the current research agendas (see App. A). The Arabic numbers refer to the 53 tasks, the Roman numerals to the three priority categories.

[8]The *character* of a problem, as used here, means its *identifying features*, whether the problem is espionage, security violations, etc. The *mechanism* of a problem means the *process* by which the consequences of the problem are realized, e.g., the negligence of authorized personnel in handling documents, which allows unauthorized personnel to gain access and transmit secrets to an enemy. If the problem were an epidemic of human illness and death, the *character* of the problem might be the plague, flu, or cholera, and *mechanisms* might be infection by rat-borne fleas or contaminated drinking water.

Task II-9 may be premature if the personnel security program requires redesign or redirection. Management information systems can improve the efficiency of a well-defined program by making more and better information available, but they cannot substitute or compensate for program design deficiencies. If the program does need reevaluation and redesign to deal with changing problems and environments, defining the information needed for managing it should await better definition of the program itself.

Task II-10 has the potential for exposing a broad set of issues that bear upon the evaluation and design of the personnel security program. If a cost-benefit framework were available for evaluating personnel security programs and proposals, it would, presumably, have to be based upon much clearer definitions of the personnel security problem, its costs, and the program's objectives, priorities, tradeoffs, and measures of effectiveness. Thus, this task, properly executed, will require laying and completing some intellectual foundations for the personnel security program that are not evident today.

Task III-28 barely touches a much broader issue: What are the alternative approaches to better personnel attitudes toward security? As presently defined, this task would explore the development of ethics "compatible with traditional American values"; but there are undoubtedly many other approaches that might be pursued, and the selection and evaluation of such approaches are utterly dependent on a clear definition of the personnel security problem. To promote better attitudes toward security, the problem has to be defined: Is it security violations (leaving safes open)? Vulnerability to enemy agents? Greed? Anger? On all of these and more? If it is all of these and more, are they all equally important? One cannot evaluate alternatives without criteria; and the criteria can be derived or supported only by definition of the problem—through explicit assumptions or facts.

Analysis of the Questions

The 176 tab questions are an expansion of nine of the ten first-priority tasks. Since all of those tasks deal with functions at the bottom two levels of the hierarchy, it seems reasonable to expect that most, if not all, of the tab questions will also deal with those same functions. However, the tab questions associated with two of the tasks deal with a wide range of topics and functions.

The tab questions can be broken down according to the same structure used in Tables 2 through 4, as shown in Table 5. The tab questions associated with Task I-4 (Tab 4) consist of two sets, one dealing primarily with monitoring (a continuing evaluation program) and the

other with investigation (periodic reinvestigation). Two of the 176 questions clearly straddled two functions and were therefore split to make the fractional entries in Table 5.[9]

The two tasks that appear to have spawned a broader set of questions are Tasks I-2 and I-5. Task I-2 is fundamental to the theory that underlies the current focus on background investigations and adjudication as a basis for the granting of security clearances:

> Validate existing criteria for personnel security clearance determinations, and develop more objective, uniform, and valid adjudication standards, e.g., develop nexus with respect to the various criteria. [I-2]

This task would probe the provable relationship, if any, between the information acquired through background investigations and security. Eleven of the 30 tab questions for this task confront some basic, unresolved issues about the security problem:

1. Does desire to succeed lead to security violations? [2-6][10]
2. Compare our hiring philosophy with that in private sector. [2-7]
3. How do private organizations, e.g., Brinks, Wall Street brokers, make decisions? [2-8]
4. Is "manipulability by others" measurable and predictive? [2-9]
5. We need a typology of security outcomes—spying, security violation, industrial espionage, theft, carelessness, PRP. [2-13]
6. What do courts, Congress, public and interest groups expect *re* nexus? [2-14]
7. How do you define security risk? [2-24]
8. Should risk be expanded from selling secrets to theft-in-general, white-collar crime, etc.? [2-26]
9. Can we develop a profile indicative of susceptibility to approach by hostile agents? [2-28]
10. Are child abuse victims security risks? [2-29]
11. Can psychological tests be used to predict security risks? [2-30]

---

[9]These two questions were Tabs 2-16 and 7-5. Question 2-16 asks, Should there be some reasons for turndowns or revocations [of clearances] for which there's no rebuttal or appeal? As such, it deals with both the denial and revoking of clearances. Question 7-5 asks, What would effects of screening-out vs. screening-in for clearances be on adjudicators? While the question derives from concerns about adjudication, it deals with a fundamental question about screening philosophy.

[10]The numbers in brackets are references to the current research agendas (see App. A). The first number refers to the task, the second to the tab question.

Table 5

FIRST-PRIORITY TAB QUESTIONS, BY HIERARCHY LEVELS

	Hierarchy Level								
	I	II	III		IV			V	
Tab	Problem	Program	Grant/Deny Clearance	Revoke Clearance	Screening	Adjudication	Monitoring	Investigation	Total
1						2		20[a]	22
2	11		1.5	1.5		15[a]	1		30
3								15[a]	15
4A		1				1	13[a]		15
4B								11[a]	11
5	6	6				23[a]	7[a]		19
6									23
7					0.5	26.5[a]			27
8								6[a]	6
9							8[a]		8
Total	17	7	1.5	1.5	0.5	67.5	29	52	176

[a]Principal topic of task associated with tab questions.

Of these, Question 2-24 poses a fundamental definitional question about the personnel security problem, the answer to which would seem essential to the design of the personnel security program. Question 2-13 could be helpful in structuring the answer, and Question 2-26 reflects uncertainty about what the answer should be. Some questions (e.g., 2-28 and 2-30) are phrased as procedural feasibility issues, but they are deeply embedded in defining the security problem.

Unfortunately, the tab questions collectively represent glancing, rather than direct, attacks on the larger question: What is the personnel security problem—in size, character, mechanisms, costs, trends, and relationship to other security problems? Since that is a difficult one to answer, even if directly addressed, it is not likely to yield to indirect questions associated with a much more concrete subject such as adjudication criteria.

The second task associated with a broader set of questions is Task I-5:

> Analyze causes and factors in security violations by cleared personnel, and develop security violations data bases. [I-5]

This task is focused on monitoring security violations, which are presumably a part of the security problem. The 19 questions associated with this task are roughly divided in thirds among the problem, the program, and monitoring.

Six of the questions are problem-oriented:

1. How big is the security violation problem? [5-1]
2. What is the distribution of incidents by agency, department, contractor, type of incident, etc.? [5-2]
3. What has been the trend in numbers and types of violations? [5-3]
4. What characteristics differentiate organizations having high and low reported violation frequencies? [5-8]
5. What is the correlation of frequency of incidence of security violations with reliability, untrustworthiness, loyalty? [5-11]
6. How many security violations are known to coworkers or supervisors but not reported? Are there patterns in these failures? If there is a problem, how do we remedy it? [5-19]

This is a remarkably complete set of questions about one presumed part of the security problem. They address the size, character, trends, and relationship of security violations to other security problems—but there are no direct questions about their mechanisms or costs.

Nevertheless, this is the best set of questions in the current research agenda about any aspect of the personnel security problem. Regrettably, they apply only to security violations, which are presumably only a part of the problem; and they lack the essential inquiry into its costs.

Another six questions associated with Task I-5 are program-oriented:

1. What is DoD's policy on reporting violations? [5-5]
2. What would managers do in terms of disciplinary steps if they had a perfect or ideal reporting system available to them? [5-7]
3. What is the role of communications security telephone monitoring? [5-10]
4. What are the punitive measures, if any, in effect to deter violators—should they be changed, improved? [5-12]
5. Who investigates violations—what are qualifications—disincentives? [5-13]
6. Do model programs exist for reporting, acting on security violations? [5-16]

Most of these questions appear to be aimed, appropriately, at defining just what the current program *is* for dealing with security violations. Perhaps the most innovative is Question 5-7: What limits effective action on security violations—the reporting system or the disciplinary system? Question 5-16 is intriguing because of its reference to "model programs." If there is an objective basis or criterion for discerning what constitutes a model program here, there must be much more than is evident to us about the problem and the program's objectives and strategy.

What is obviously missing from this set of six questions about the program for dealing with security violations is any attempt to measure either cost or effectiveness. Such measurements, of course, depend upon the definition of the problem and the setting of program objectives against which effectiveness can be measured. Given all of those things—a defined problem, program objectives, and measures of current program cost and effectiveness—the next set of questions should deal with alternative approaches that can be evaluated against the current program on the basis of cost and effectiveness.

The only other question that falls into the upper two levels of the hierarchy is one associated with Task I-4. The task is stated as:

> Analyze efficacy of current continuing evaluation programs, e.g., is the periodic investigation a good deterrent? [I-4]

The question associated with it is:

> What is the interrelationship between security posture at front end, i.e., initial hiring, and continuing evaluation programs? [4-A8]

This is one of the very few questions anywhere in the current research agendas that deals directly with tradeoffs between internal elements of the personnel security program—tradeoffs that are important to the design and balancing of the program for least cost or greatest effectiveness. This question asks about the tradeoffs between the program efforts devoted to the initial hiring (i.e., screening) and the monitoring of personnel after hiring. The same question should be asked of the tradeoffs between investigation and adjudication, between denying and revoking clearances, between security violations and espionage, and so forth throughout the program. And then outside the program: What are the tradeoffs between the personnel security program and those for physical security, information security, counterintelligence, etc.

ANALYSIS OF THE AGENDAS BY SUBJECT

The preceding analysis has viewed the current research agendas as a whole, seeking structure, emphasis, patterns and anomalies. Appendix C provides a narrower-scope examination of the agendas *within* the context of the subject they address. The questions explored there are more limited: Given that the current research agendas address this particular subject, are there any obvious gaps and, if so, what should fill them?

ANALYTICAL ASSESSMENT OF THE AGENDAS

The current research agendas appear to have several imbalances. They are devoted to:

- Means more than ends.
- Existing more than alternative means.
- Supporting more than questioning theories.
- Designing more than evaluating procedures.
- Elaboration or details more than guiding principles or concepts.
- Procedural improvements more than problem understanding.

The most obvious omissions in the agendas, even within their treatment of any subject or topic, are:

- Costs of the personnel security problem or program or its elements.
- Tradeoffs among procedures, operations, and activities, even within the personnel security program.
- Alternatives to the current procedures, operations, activities, theories, etc., that now define the program.

Whether those imbalances and omissions are intended or desirable involve questions that lie outside the agendas themselves. But the directions of the imbalances and the nature of the omissions would suggest to an outside observer that the personnel security problem is well understood, that the program is well designed to address it, and that research is required mainly to "fine tune" some of the procedures.

IV. ADDITIONAL RESEARCH AGENDAS

INTRODUCTION

Research can have several purposes. As conventionally defined, *research* is diligent and systematic inquiry or investigation into a subject to "discover or revise facts, theories, applications, etc."[1] Thus, the purpose of personnel security research could be to learn more about the personnel security problem; to provide a basis for changing the personnel security system to reflect the changes in the personnel security problem in recent years; or to change the details of elements of the current personnel security program.

Although the report of the Stilwell Commission does not call for research in these terms, the concern of the Commission with the need for research having a range of purposes is clear and clearly consistent with this definition.

The general assessment of the Stilwell Commission was that "the DoD security program has been reasonably effective," but the Commission also noted that the current program "falls short of providing as much assurance as it might" and that the primary "challenge [to keeping the nation's secrets] is people," not technical problems.[2] It further noted that "although billions of dollars are spent annually for security, relatively little goes to research activities," in particular, to those "significant aspects of policy and practice which should properly be based on research."[3] Stated differently, it was the opinion of the Stilwell Commission that there are worrisome deficiencies in security that center on personnel, and research should not be limited simply to the details of current security programs, i.e., current "practice." Personnel security "policy" itself should also receive research attention.

Our assessment supports this general conclusion and suggests specific areas where such research seems needed as a first order of business.

Our efforts to identify definitive statements and descriptions of the personnel security problem, program objectives, and strategy have included both literature searches and discussions with experienced

---

[1]*The Random House Dictionary of the English Language*, Random House, New York, 1966.

[2]*Keeping the Nation's Secrets: A Report to the Secretary of Defense by the Commission to Review DoD Security Policies and Practices*, Office of the Secretary of Defense, November 19, 1985, p. 7.

[3]*Keeping the Nation's Secrets*, op. cit., p. 86.

security personnel. They have not been successful to date. In the following three subsections we discuss each of these three missing elements in turn and propose agendas of research to supply some of the needed information.

THE PERSONNEL SECURITY PROBLEM[4]

Issues

The appropriateness of—or, even more, the requirement for—a careful and comprehensive statement of the problem for which a solution is to be sought is not always appreciated. First of all, as others have noted, simply "identifying a situation as problematic does not carry problem solving very far."[5] Moreover:

> It is a familiar and significant saying that a problem well put is half-solved. To find out *what* the problem and problems are which a problematic situation presents to be inquired into, is to be well along in inquiry. To mistake the problem involved is to cause subsequent inquiry to go astray . . . . The way in which a problem is conceived decides what specific suggestions are entertained and which are dismissed; what data are selected and which rejected; it is the criterion for relevancy and irrelevancy of hypotheses and conceptual structures.[6]

A careful statement identifying and describing the problem is important as a starting point precisely because it provides a focus for the details of the solution. If the problem is too narrowly defined, the solution may be appropriate but will relieve only a portion of the original difficulties. If the problem is incorrectly defined, the situation will almost certainly be at least partially inappropriate and of disappointing effectiveness.

Two different kinds of issues arise in connection with statements and descriptions of problems to be solved. The first can be called the definition or boundary problem because it is concerned with distinguishing between what is and what is not part of the problem. The second is concerned with providing enough substance and structure in the description of the problem to guide efforts to solve it. Both of these aspects of the personnel security problem are discussed below.

---

[4]For the purposes of this report we use the standard dictionary definition of *problem* as "a situation requiring action." That is, a problem is not just a situation to be endured.

[5]Arthur D. Hall, *A Methodology for Systems Engineering*, D. Van Nostrand Co. Inc., Princeton, New Jersey, 1962, p. 93.

[6]John Dewey, *Logic, The Theory of Inquiry*, Henry Holt and Co., New York, 1938, cited by Hall, op. cit., p. 93.

As noted in Sec. II, the personnel security problem is not sharply defined, i.e., the *boundary* is not clearly and consistently drawn in practice today. If the problem is defined narrowly to focus solely on the loss of secrets through disloyal personnel, the more excluded factors lie outside the boundary that arguably should or must be included. When the problem is defined more broadly, it becomes difficult to find its core, or to separate it from problems traditionally associated with personnel management.[7]

Although persons with access to classified information are, by the definition of classified information, in a position to cause damage to the national interest, there are a variety of ways in which persons without access to classified information can also damage the national interests. A DoD program to deal with this aspect of personnel suitability or personnel management is therefore also appropriate, if not mandatory. There is little doubt, however, that the problem of the compromise of classified information is the more serious, if not the larger, problem.

We believe that the aggregation of personnel measures appropriate for keeping the nation's secrets both differs from and is larger than the aggregation of measures appropriate for selecting and retaining suitable civilian employees and military personnel. There might be no objection to combining these two programs under the *personnel security* rubric *if* their differing implications remained visible and neither program suffered or was neglected as a consequence of being combined with the other.[8] These conditions are not met, however, when the composite personnel security problem is defined in terms such as "acquiring and retaining personnel and granting clearances consistent

---

[7]The expression *personnel security* itself is not formally defined in places where such a definition might reasonably be expected. For example, the *Dictionary of Military and Associated Terms*, (Department of Defense, Joint Chiefs of Staff, JCS Pub. 1, 1979) defines such terms as *electronic security* and *physical security*, but not *personnel security*. Nor is the expression defined in the DoD regulation defining the DoD personnel security program (*Personnel Security Program*, Department of Defense, Office of the Deputy Under Secretary of Defense (Policy), DoD 5200.2-R, January 1987). This regulation does define *personnel security investigation*, from which a definition of *personnel security* can be inferred, but the inferred definition is broad and diffuse.

[8]R. V. Jones traces Britain's failure to have bulletproof aircraft fuel tanks in the early days of World War II—even though a nearly satisfactory bulletproof tank had been developed before the end of World War I—to unsatisfactory definition of the problem. When World War I ended, the peacetime problem became crashes, not bullets, so designers tried to make fuel tanks crashproof as well as bulletproof. "As a result, every design submitted to the Air Ministry was taken to Farnborough, filled with liquid, and dropped over the side of one of the buildings onto concrete, where it inevitably broke up . . . , none could stand the fall of 60 ft. onto concrete." (*The Wizard War: British Scientific Intelligence, 1939-1945*, Coward, McCann & Geoghegan, Inc., New York, 1978, p. 78.)

with the interests of national security," as in the current DoD personnel security program. For example, Termination Briefings, which are included in the current program because their importance is widely appreciated, in fact have no logical role to play in either "acquiring and retaining personnel" or "denying, granting or revoking clearances," whereas they do have a role in "keeping the nation's secrets." Termination Briefings are included in spite of, not because of, the way the problem is defined. Thus, the definition problem is important; the boundary must be drawn with care.

The *content description* problem can be discussed at two levels, that of descriptive details and that of theory or structure.

The essentiality of a comprehensive description and explicit awareness of all the relevant aspects of the personnel security problem is perhaps the easier level to demonstrate. Consider for the moment just that part of the personnel security problem that is concerned with the compromise of classified information through the actions of spies. To provide enough information to develop an adequate personnel security program, it is necessary to know a large number of details about the entire process of compromise. For example, if it were not known that some persons become spies while on the job as a consequence of changes in their private lives after they successfully passed their preclearance investigation, there would be no logical role for periodic reinvestigations of the same type as the preclearance investigation (unless it is assumed that the investigators conducting the preclearance investigation had not done their job properly).[9] It would be more logical to conclude that all that was needed was to improve the preclearance investigations.

In the same way that knowing *when* a person becomes disloyal makes a difference to the personnel security program, it would seem that knowing *how* a person becomes disloyal should also make a difference. For example, it appears to be true that persons become spies by at least three different means: self-recruitment and both "crash" and "gradual" recruitment by foreign intelligence officers.[10] The DoD personnel security program should in some way reflect this information, yet it does not. Does this gap mean that the information was simply overlooked when the DoD program was developed? Or was that partic-

[9]Whether or not periodic reinvestigations are the preferred solution to the problem of persons becoming spies on the job is another question; the point here is that that *is* the justification for periodic reinvestigations.

[10]Victor Suvorov, the pseudonym of a GRU defector, describes GRU use of both "crash" and "gradual" recruitment in *Inside Soviet Military Intelligence*, Macmillan, New York, 1984, pp. 116–118, and John Barron describes KGB use of the "gradual" three-step spotting, cultivating, and "hooking" process in *KGB: The Secret Work of Soviet Agents*, Reader's Digest Press, New York, 1974, pp. 193–194.

ular fact very well known and considered explicitly when the program was developed, but had no effect on the ultimate program because it could not be usefully exploited? And how can anyone tell in retrospect without an explicit description of the problem that existed at the time the program was developed?

The potential utility of extending the description of the personnel security problem beyond the simple aggregation of facts to include the development and analysis of theories can be illustrated by building upon the above example. The processes of interest here are the processes of inductive and deductive reasoning that are the hallmark of the scientific method. The process of induction implies reasoning from particular facts to a general theory or conclusion. The process of deduction then implies reasoning from the general theory or conclusion, a process of inference. One application of this method of potential interest here would be the development of theories of the spy from detailed knowledge of the sort suggested above, and then an examination of the policy implications of those theories.

As a specific example, consider the following list of seven possible theories of espionage, each of which is supported to varying degrees by the available evidence.[11] For purposes of discussion, we supply each theory with a suggestive name and provide a very brief description:

- *Foreign preference theory*: Espionage results from personnel whose loyalties, interests, or preferences are opposed to those of the United States.
- *Trait theory*: Unreliability is latent in one's personality but is detectable through related tendencies in past behavior.
- *Ties theory*: Individuals function within a framework of loyalties, obligations, shared objectives, ties, and goals that are dependent upon others—all of which bind the individual to other people and institutions. These can be manipulated to gain influence or to coerce.
- *Event* or *situation theory*: Individuals have characteristics that can be affected or triggered, or reliability thresholds that can be exceeded, by certain events, situations, and environments in work and personal affairs.
- *Incentive theory*: Disloyalty will occur when expected benefits exceed expected risks.

[11]This list is adapted from unpublished research by Rae Starr, one of the authors of this report. Chapman Pincher uses a somewhat different approach to developing theories in his *Traitors: The Anatomy of Treason*, St. Martin's Press, New York, 1987, pp. 276–278.

- *Expectations theory*: Individuals may become disloyal if it becomes apparent that their loyalty has not served their long-term interests.
- *Moral ambiguity theory*: Situations may offer rationalizations that remove barriers to disloyalty.

Although we make no claim that this list is complete or that it is the best that could be compiled, we observe that certain types of conclusions can be drawn after the detailed data have been generalized into theories:

1. Regardless of whether or not there are exactly seven (or six or eight) distinctive theories of espionage, it is clear that espionage can occur for a variety of reasons. Personnel security policy can not be based on the assumption that espionage has only a single cause or explanation. And if there are several plausible theories of espionage, it is necessary to be explicit about their relative credibility, importance, occurrence, and, therefore, weight in policymaking.
2. Different theories have different policy implications. *Foreign preference* theory suggests the utility of background checks for citizenship, memberships, and affiliations, even if such checks are totally worthless for reliably detecting indicators of undesirable traits. *Incentive* theory suggests programs to monitor for wealth or other selected indicators after employment has begun. The other side of the coin of *incentive* theory suggests that unwittingly "hooked" but as yet undetected agents might be induced to cease their acts of compromise by an appropriate balance of threats and promises.
3. Different theories suggest different research questions. *Trait* theory highlights the "nexus" question: What, if any, behavior, personality, or character traits are indisputably linked to latent disloyalty? *Expectations* theory suggests the utility of research on programs to identify expectations during hiring, to influence expectations during career guidance, and to monitor expectations during performance reviews. If, as suggested in item 2 above, *incentive* theory suggests the possibility of retrieving unwittingly hooked agents, it also suggests research on the content of a balanced "carrot and stick" program that could encourage the required admission of activities by the agent without appearing to tolerate or reward the initial espionage.[12]

[12]Some of the examples cited in this and the accompanying paragraphs are well-known and others are not. For example, the detection of foreign preference has always

This list of conclusions is far from complete, of course, as are the examples included here. One of the purposes of research on theories of the personnel security problem is to identity the potential extent of the problem and the full range of potential opportunities that address it.

A PROPOSED AGENDA OF RESEARCH

We propose the following specific tasks as a starting point for new research on the nature of the personnel security problem. This list is obviously not complete; other tasks could be formulated now, and still others will suggest themselves as the research progresses:

1. Describe the features of the personnel security problem that distinguish it from other aspects of the larger problem of keeping the nation's secrets and from the issue of personnel suitability.
2. Develop a comprehensive model or description of the ways by which the nation's secrets are lost—including both deliberate compromise and security violations, for example—identifying the major features of each, such as means of spy recruitment and channels for the compromise of classified information.
3. Develop a comprehensive theory or set of theories of the spy that describe when, why, and how an individual becomes disloyal.
4. Identify the actual peacetime costs and the likely wartime consequences of the personnel security problem as it has developed in recent years.
5. Identify the costs of all elements of the current DoD personnel security program.
6. Identify and assess the effectiveness of the elements of current and past personnel security programs that are responsive to distinguishable elements of the current personnel security problem.
7. Develop procedures for assessing the effectiveness of tradeoffs in the allocation of resources among personnel security programs and the programs of other security disciplines having the same goal, i.e., protecting the nation's secrets.
8. Compare the DoD personnel security program with the personnel security programs of other nations and other organizations with significant personnel security problems.

---

been a goal of background checks. On the other hand, nothing in the current DoD personnel security program addresses the agent engaged in compromise, regardless of how he became an agent.

OBJECTIVES FOR THE DoD PERSONNEL SECURITY PROGRAM[13]

Issues

A concise statement of the objective of concerted activity is useful because it provides:

- Guidance for the selection of a strategy and the development of programs to solve problems.
- Criteria by which the success of the programs can be judged.

Although the appropriateness of a careful statement of the objective may be obvious, there are at least two different issues involved.

The first issue concerns the choice of the objective itself. The importance of care in this choice can be illustrated by the historical example of antiaircraft guns mounted on merchant ships in World War II. This tactic was initially judged to be not worth the cost because very few attacking bombers were shot down. However, the true objective of the guns was not to destroy bombers, but to keep ships from being sunk by bombers. The antiaircraft guns were judged to be well worth the cost in terms of their success in achieving this objective. Although the antiaircraft crews were seldom well-enough trained to shoot down many bombers, far fewer armed ships were sunk.[14]

The second issue is related but emphasizes the words used to express the objective. To illustrate this point, consider the well-known expression, "If a man builds a better mousetrap, the world will beat a path to his door":

> The first thing to do, however, is to make sure that we know exactly what . . . goal we are trying to reach. I think that we can decide right at the start that our goal is not to have a path beaten to our door, but it might not be quite so easy to decide that our goal might not be building a better mousetrap either. Actually, our prime goal is to get rid of mice in some way or another, and when stated in this way we don't care whether we trap them, electrocute them, drown them, or scare them to death—anything to get rid of them. The words you use . . . have to be chosen very carefully so that the referents of these words or their connotations do not limit the thinking . . . [of the person] to whom you assign this task. The wrong word can unintentionally predispose the thinking . . . to follow a lim-

[13]For the purpose of this discussion, we use the conventional dictionary definition of *objective* as "something one's efforts are intended to accomplish or gain, i.e., a purpose, goal or target."

[14]See Philip M. Morse and George E. Kimball, *Methods of Operations Research*, The Technology Press of Massachusetts Institute of Technology and John Wiley & Sons, New York, 1st Ed., Rev. 1951, pp. 52–53.

> ited number of paths and preclude . . . investigation of other equally desirable and fruitful ones.[15]

Both of these points are relevant in the area of personnel security. In addition, the current personnel security problem is not a single problem but a cluster of several problems. Choosing an appropriate statement of objectives to guide such composite personnel security programs is thus further complicated.

To illustrate some of the complexities involved, consider the choice of an objective for that part of the personnel security program that addresses disloyal personnel deliberately compromising classified material (as distinct from security violations that do not lead to compromise of classified material, and from personnel suitability problems that do not involve classified material at all).

If the focus of the statement of the problem is on *personnel with access to classified material* who are or might become disloyal, it might be appropriate for the objective of the personnel security program to focus on access, i.e., on granting, denying, and revoking clearances. If, on the other hand, the statement of the problem focuses on the *compromise* of classified information, then a personnel security program that is concerned only with clearances is clearly inadequate because it does not even address the problem. Clearances are a means to the end of keeping secrets, not the end itself. Denying clearances to persons who are known to be agents of the Soviet Union or who are judged likely to become agents is one way to preclude the opening of channels for unauthorized transmission of classified material. Similarly, revoking the clearance of a known agent is one way to close a known existing channel. But neither of these actions is relevant to the unknown agent, who should be of at least equal concern.

The entire burden of keeping the nation's secrets does not fall on the personnel security system, of course. Neither does the entire burden of seeking to detect and close channels of transmission that exploit agents. But since personnel are involved, the problem is or should be of concern to the personnel security program. The undetected agent is the essential link in the unauthorized disclosure of classified information. He is obviously in an ideal position to interrupt that flow. But his cooperation must be gained, and this may be possible in many cases. As noted above, many agents apparently become involved unwittingly in a process in which they are spotted, then cultivated, and finally "hooked" over a period of time in a sequence of seemingly in-

[15]Hall, op. cit., p. 94.

nocuous actions.[16] In addition, some agents apparently regret their involvement at some stage, as Jerry Whitworth asserted in his first letter to the FBI that he did when he discovered that the Soviets were the beneficiaries of his actions.[17] It is not immediately obvious how agents could be encouraged to "break" with their controller (with or without becoming informers), but the point is that this is a reasonable concern for the personnel security program. More important, however, issues such as this will never even be considered in a personnel security program that views its objective solely as "granting, denying and revoking clearances in the national interest." Further research on objectives appropriate for the DoD personnel security program is at least as urgently needed as is research on improving the process of granting clearances.

A Proposed Agenda of Research

We propose the following specific tasks as a starting point for new research on objectives for the DoD personnel security program. Again, the list is not complete. Other tasks could be formulated now, and still others will suggest themselves as the research progresses:

1. Develop and describe alternative candidate statements of objectives for the DoD personnel security program.
2. Assess the advantages and disadvantages of statements of objectives for the DoD personnel security program that focus on the granting, revoking, and denying of clearances.
3. Develop and assess the advantages and disadvantages of alternative statements of objectives for the DoD personnel security program that focus on motivating or influencing the attitude and behavior of persons with clearances.
4. Develop and assess the advantages and disadvantages of alternative statements of objectives for the DoD personnel security program that focus on the classified material at risk of being compromised.
5. Develop and assess the advantages and disadvantages of other statements of the objectives for the DoD personnel security program identified in item 1 above.

---

[16]The William H. Bell case, for example, which developed in this fashion, has been described as "a classic example of the recruitment of cleared U.S. personnel for espionage by hostile intelligence operations." (*Recent Espionage Cases: Summaries and Sources*, Department of Defense Security Institute, January 1987, p. 5.)

[17]John Barron, *Breaking the Ring*, op. cit., p. 4.

STRATEGY FOR THE DoD PERSONNEL SECURITY PROGRAM[18]

Issues

The primary utility of a clear statement of strategy is that it provides guidance for the development of programs to achieve established objectives by identifying the preferred method or approach and by making clear the difference and the relationship between means and ends. Thus, strategy cannot be independent of the problem or of the objectives that have been established. To illustrate, consider the personnel security situation as it was perceived in the early 1950s:

In 1953, when President Eisenhower signed Executive Order 10450, the prevailing view of the personnel security problem was that classified information was being compromised by persons who had become overt members of the Communist party or Communist sympathizers in the 1930s or during the wartime alliance between the United States and the Soviet Union.[19] Thus, one objective of the personnel security program at that time was to ensure that "all persons privileged to be employed in the departments or agencies of the Government shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States."[20] To meet that objective, it was required that "the appointment of each civilian officer or employee in any department or agency of the Government shall be made subject to investigation."[21] Of course, that strategy rested on one or more implicit (and, in retrospect, rather heroic) assumptions:

- A preemployment investigation can screen out not only Communists but others who are inherently unreliable, untrustworthy, etc.

---

[18]As before, we use the dictionary definition of *strategy* as "a concept relating means to ends; a plan, method or approach for combining and employing specific or available means to achieve specified ends, given a specific problem."

[19]"Alexander Orlov, the highest ranking Soviet Intelligence official ever to defect to the West, told a senate committee that in his time (the 1930s) about 60 percent of the most efficient Soviet spies were Communists, and the Communists were supposed to work for their spiritual fatherland, for Russia, and not for money." (Walter Laqueur, *A World of Secrets: The Uses and Limits of Intelligence*, Basic Books Inc., New York, 1985, p. 25.) Laqueur goes on to note that "for the 'typical' Soviet spy in the . . . post-Philby generation, mercenary motives or weakness of character seem to have been far more important."

[20]Executive Order 10450, "Security Requirements for Government Employment," first paragraph of preamble. A copy of this document is included in *Federal Government Security Clearance Programs: Hearings Before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs*, U.S. Senate, 99th Cong., 1st Sess., S. Hrg. 99-166, p. 43.

[21]Executive Order 10450, Sec. 2.

- All employees of the government will be reliable, trustworthy, etc., if Communists and Communist sympathizers are denied employment.

But that strategy would be appropriate only as long as:

- The problem and objective were correctly described and remained unchanged.
- The assumptions of cause and effect that support the strategy are valid.

Today, it is generally recognized that the problem of compromise is not limited to persons who become disloyal before the mandated preclearance investigation. An individual can "turn" while on the job, years after becoming a government employee, or even after he has left the employment that gave him access to classified information. A strategy that includes periodic reinvestigation therefore suggests itself (particularly since Soviet intelligence officers will be actively working to turn cleared individuals with access to classified information). A strategy of investigation and periodic reinvestigation is clearly superior to a strategy limited to a single investigation, but it, too, will become increasingly inadequate as the interval between investigations lengthens.

The addition of periodic reinvestigation is a *modification* to, or adaptation of, the strategy of initial, preemployment investigations. If the problem of people "turning" on the job had been perceived at the outset as being more serious than that of inadvertently hiring Communists, a strategy focused on investigations might not have been preferred over one oriented, say, toward the continuous monitoring of employees. Thus, the initial perception of the problem may have led to the adoption of a strategy that was subsequently modified rather than changed as perceptions of the problem changed—with the possibility that the modifications may be less effective than a new approach to the problem.

The wording of the objective in Executive Order 10450 probably did not help matters. The phrasing of the Order appears to be inadequate as a statement of the program objective. The objective of that part of the personnel security program concerned with the compromise of classified information should have been phrased something like "to prevent, preclude or minimize such compromise," rather than "to ensure loyal personnel."

One might see the differences between the two phrases as superficial or inconsequential. After all, the latter objective would be met, i.e., compromise would not occur, if "all persons privileged to be employed

in the departments or agencies of the government [were] reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States." So aren't the two essentially equivalent?

That they are not equivalent can be easily demonstrated. "Complete and unswerving loyalty to the United States" is an impossible objective. It is certain that the loyalty of some persons with access to classified information will be something less than complete and unswerving.[22] If the objective is "complete and unswerving loyalty," there is no reason to seek to protect classified information; if the objective is to "minimize the compromise of classified information," seeking loyal personnel can be one means to that end, along with other personnel security measures to protect classified information if disloyal persons might have access to that information.

Furthermore, pursuit of a strategy limited solely to preclearance investigations in the face of possible future disloyalty problems requires that the investigations have predictive capabilities, which is unrealistic. Expanding the strategy to include periodic reinvestigations is clearly an improvement, in that it provides a potential opportunity to detect any adverse overt change since the last investigation; however, depending on the interval between investigations, it may still permit many years of uninterrupted compromises.

The current approach emphasizing initial investigation and periodic reinvestigation is of sufficiently limited utility to warrant serious research into new strategies. We cannot specify what the best strategy might be, but we know enough to suggest three possible elements: preclearance investigations, monitoring, and "reconciliation" efforts. Each of these is discussed briefly below.

Preclearance investigations are obviously appealing because, if they were completely effective, they could essentially nip the compromise problem in the bud. When the espionage problem has persisted, suggesting that past investigations have not been good enough, it has been tempting to believe that it is only necessary to improve the investigations in some way and the problem will be solved. Preclearance investigations clearly have some utility, but they also equally clearly have limitations:

- Clearances obviously should not be granted to persons who openly declare their allegiance to foreign countries. Preclear-

[22]This raises questions about the wisdom of selecting unachievable objectives, given their predictably undesirable consequences—such as the failure to achieve a perfectly feasible objective, the inevitable misallocation of resources if the objective is taken seriously, or the fostering of cynicism.

ance investigations presumably can detect overt prior expressions of foreign preference. The ability of preclearance investigations to detect covert foreign preferences is more doubtful.

- Several different kinds of "clear risks" can be identified. These include the inability to establish identity bona fides, vulnerability to coercion, and demonstrated mental or emotional instability. Part of understanding the espionage problem includes knowing that the Soviets seek to introduce "illegals" into the United States for any of several reasons. We should not grant access to classified material to any individual who cannot prove his or her identity. The Soviet willingness to exploit familial or emotional relationships between persons within their grasp and persons with clearances also has obvious implications for denying clearances to persons with such linkages. Finally, there would seem to be an *ipso facto* argument against granting clearances to people with mental or emotional instabilities, from whatever source. And there may be other equally obvious "clear risks" that could be detected by suitable investigations.
- Preclearance investigations may be quite effective in detecting a number of other character or behavior traits whose relevance to personnel security is not as obvious as the "clear risks" identified above, e.g., criminal records, alcohol and substance abuse, spouse and child abuse, and sexual perversion. Although such problems, which may be detected by preclearance investigations, are widely accepted as relevant to a determination of general suitability for employment, their relevance to security issues is more contestable. It depends on theories more than unambiguous facts. If those theories are to be relied upon, they should be made explicit and should be validated through research.
- Finally, to the extent that the problem of compromise involves persons who were completely loyal when they were initially cleared but became disloyal as a consequence of changed conditions, preclearance investigations have no utility whatsoever unless some detectable personality or character traits can be identified that are reliable predictors of changed conditions and subsequent disloyalty. We know of no responsible claims for the existence of such indicators or predictors.

Thus it seems clear that preclearance investigations have a useful but limited role to play. Certainly, their role should not be the dominant or exclusive strategy in the personnel security program.

The prospects for periodic reinvestigations appear to be quite similar, but with one important difference. A person with access to

classified information presumably would have more knowledge and awareness of security programs and procedures than a person who had never been cleared for such access. If a cleared person were to decide to compromise information in his possession, he would almost certainly attempt to avoid or conceal his disloyalty, thereby reducing the likelihood of detection by a periodic reinvestigation.

Even less can be said with certainty about a possible strategy of selective but continuous monitoring of persons with access to classified information. At least two distinct alternatives can be identified, however:

1. In the same way that specific items can be identified for attention in an investigation, specific items can be identified for monitoring. The items on this list could be selected from a list of indicators compiled from analyses of past espionage cases, e.g., financial statements, for evidence of unexplained affluence; medical records, for evidence of mental and physical difficulties; credit records, for evidence of overindebtedness; personnel records, for evidence of job dissatisfaction or alienation; police and court records, for evidence of disregard for law.
2. Monitoring could be designed simply to detect changes in the conduct or condition of persons involved, without specifying in advance the types of change of concern. A behavioral or personality change in an individual would not necessarily be evidence of espionage, of course, but it could serve as a signal of the need to conduct a more specific investigation.

Who should do such monitoring, whether the evidence from past espionage cases justifies statistical inferences on these aspects or whether such monitoring is excessively intrusive are good questions for research. It should not be *assumed* that such questions are settled and that "research" to develop implementing procedures is warranted.

Preclearance investigations and monitoring on the job are two complementary approaches to personnel security. But a third one, which we call "reconciliation" for want of a better term, and probably others as well should be considered. While investigations and monitoring would seek to prevent the opening of new channels for unauthorized access, approaches are also needed to close existing channels. Monitoring might help, as would revoking the clearance of known spies. Counterintelligence efforts are designed in part to detect unknown channels; but the undetected agent is the heart of the undetected channel of compromise. Gaining his cooperation will close an undetected channel.

Although perhaps not applicable in all circumstances, a strategy of reconciliation may be effective for those agents who unwittingly become "hooked" or for those who at some later time regret their participation.

Our general conclusion is that the strategy of the personnel security program should be explicitly studied to determine which element or combination of elements offers the best prospects for achieving the objectives of the program.

A Proposed Research Agenda

The following tasks are proposed as a starting point for new research on strategies to achieve the objectives of the DoD personnel security program. Again, the list is not complete. Other tasks could be formulated now, and others will suggest themselves as the research progresses:

1. Develop and describe possible alternative strategies for achieving the objectives of the DoD personnel security program.
2. Describe and assess the capabilities and limitations of strategies employing investigative programs for achieving the objectives of the DoD personnel security program.
3. Develop, describe, and assess the feasibility, capabilities, and limitations of strategies that focus on monitoring personnel with access to classified material as a means of achieving the objectives of the DoD personnel security program.
4. Develop, describe, and assess the feasibility, capabilities, and limitations of strategies that focus on motivating undetected spies to cease spying and/or to cooperate with counterespionage authorities as a means of achieving the objectives of the DoD personnel security program.
5. Develop, describe, and assess the feasibility, capabilities, and limitations of other strategies identified in item 1 above as a means of achieving the objectives of the DoD personnel security program.
6. Develop procedures for assessing the effectiveness of tradeoffs in resource allocation within the DoD personnel security program among such elements as investigation, adjudication, and monitoring.

V. CONCLUSIONS AND OBSERVATIONS

The problem of deliberate compromise of classified information by persons trusted with access to it is extremely serious.[1] The costs and consequences of this problem are somewhat uncertain, but they include high actual peacetime costs and alarming potential wartime consequences. A perfect or near-perfect system to prevent the loss of a nation's secrets generally or to prevent the compromise of classified information by disloyal persons is almost certainly beyond reach. Nevertheless, the problem clearly warrants determined efforts.

The context in which this security problem exists is complex. The quantity of information that needs protecting is large and growing; theft or unauthorized access is probably becoming easier; a variety of conflicting national interests, issues, and values are intertwined; and societal attitudes seem to be increasingly nonsupportive.

The personnel security discipline—the measures appropriate to deal with the problem of deliberate compromise of classified information—is only one of a family of security disciplines. Others are information security, physical security, counterintelligence, technical surveillance countermeasures, and operations security. There is no way to view and assess the relative strengths and capabilities of the members of this family of security disciplines, or to judge the relative merit of additional emphasis on personnel security.

From our perspective, the conceptual framework of the DoD personnel security program appears to be largely absent or in disarray:

- The expression "personnel security" is not even defined.
- There is a blurring of security and suitability issues.
- The program is essentially activity oriented rather than problem-oriented.
- The program emphasizes clearances (and investigations) primarily for reasons of history and pragmatism, not theory or reasoned choice.
- The models and paradigms for the investigation, adjudication, and clearance process are implicit and unvalidated.

Because of these shortcomings, security suffers and the program is vulnerable to valid criticism when exposed to public view, an inevitable

[1]It is less clear that the *unintended* compromise of classified information by persons with clearances is also a serious problem; but that problem is clearly included within the broad aspects of the personnel security program.

prospect, given the probabilities of security failures associated with personnel.

The current PERSEREC program is directed primarily toward improving the existing procedural elements of the DoD personnel security program. The planned research focuses on identifying and designing additions to current activities, rather than understanding the problems, testing the validity of current theories, or exploring totally new approaches to the problems.

It is highly unlikely that a significantly improved program will result from piecemeal efforts to improve individual elements of the current program. While we recognize that PERSEREC has incentives to be responsive to the current program,[2] we would argue that a significant share of their research should be devoted to fundamental questions that underly the basic approach toward personnel security. The foundations we believe to be essential to the sound design (or redesign) of the personnel security program include:

- Clear definition of personnel security problems, including their nature, costs, and trends, and explicit assumptions about their causes.
- Explicit concepts to address those problems, including research and validation testing.
- Consideration of alternative objectives for the personnel security program and their implications for national security and other security-related programs.
- Evaluation of alternative personnel security approaches or strategies, including their costs, effectiveness, and internal and external tradeoffs.
- The design of programs and policies for personnel security that reflect explicit priorities for both ends (objectives) and means (activities).

It is almost certain that the DoD program could benefit significantly from a fundamental rethinking and restructuring. That fundamental rethinking and restructuring is not included in the current research agendas.

The question we would pose to DoD personnel security policymakers is this: Do you want the research efforts to improve personnel security

[2]PERSEREC was established under a directive (DOD 5210.79) that includes a "sunset clause" calling for its "disestablishment on September 30, 1990, unless the Executive Agent [the Secretary of the Navy], in consultation with the DUSD(P), directs its continued existence." Thus, PERSEREC must establish its contribution to the community it serves (the personnel security professionals) within that time period to justify its continued existence. That, naturally, places a premium on contributions to the current system.

to be devoted to repairing or to rebuilding the program? If the answer is both, then what balance should be struck between the two? Whatever the answers to these questions, three balances within the research agendas must be clarified:

1. The balance between basic and applied research.
2. The balance between research on procedures and on policies.
3. The balance between research to repair and research to rebuild the personnel security program.

If those balances admit *any* basic research on policies to rebuild the program, then we would urge that such research efforts initially emphasize:

- Definition of the personnel security problems.
- Separation of personnel suitability and security issues.
- Understanding of the tradeoffs internal and external to the personnel security problems and program.
- Setting priorities and selecting criteria for assessing the effectiveness of the program.

Appendix A

CURRENT RESEARCH AGENDAS

INTRODUCTION

Reproduced below are the 53 task statements that constitute the "current research agendas." These tasks were originally defined in May 1986 by a committee meeting at the Xerox Training Center in Leesburg, Virginia. They were proposed as an agenda for personnel security research to be undertaken by PERSEREC as resources would permit.

The agendas are divided into three priority categories. The first category consists of the ten tasks that were to be pursued first in the PERSEREC research program. The second category consists of another ten tasks to be pursued after the first ten have been adequately funded and initiated. The third category consists of the remaining 33 tasks, which were considered to be less cost-effective research investments than those in the first two categories.

The original agendas have been slightly modified (e.g., one task from each of the first two categories have been switched), but the changes do not materially affect the RAND analysis.

Nine of the ten first priority tasks were further developed or expanded in sets (or tabs) of questions, producing a total of 176 research questions. These questions are also reproduced here, following the 53 task statements.

53 RESEARCH TASK STATEMENTS

Priority I Research Efforts

I-1. Compare/contrast results of interview-oriented background investigation (IBI) and the special background investigation (SBI).

I-2. Validate existing criteria for personnel security clearance determinations, and develop more objective, uniform, and valid adjudication standards, e.g., develop nexus with respect to the various criteria.

I-3. Investigate the design of the investigative interview—sequencing of questions, etc.—determine how open and honest

individuals are when they are interviewed by DIS investigators, and how to improve upon openness and honesty of those interviewed.

I-4. Analyze efficacy of current continuing evaluation programs, e.g., is the periodic investigation a good deterrent?

I-5. Analyze causes and factors in security violations by cleared personnel, and develop security violations data bases.

I-6. Analyze factors causing differences in negative adjudication rates among agencies and types of applicants.

I-7. Identify relevant qualifications, characteristics, and capabilities of adjudicators, and develop selection and training guidelines for adjudicators.

I-8. Bring automated data bases, e.g., Defense Manpower Data Center's (DMDC), financial, travel, health, etc., to bear on investigations.

I-9. Run records of cleared personnel against financial data bases to determine whether problems exist—develop a system for use with people in sensitive positions.

I-10. Analyze productivity and effectiveness of current personnel security information collection procedures and information sources, e.g., neighborhoods, schools, peers, roommates; written inquiries to employers.

Priority II Research Efforts

II-1. Evaluate the Services' prescreening procedures, e.g., the Army's MEPS questionnaire and the Navy's preservice drug and offensive history inventory.

II-2. Collect and analyze personal history and behavioral data for known espionage cases to determine if they show behavioral patterns that could have led to their early detection.

II-3. Develop automated data systems insuring that information about people who lost clearances, had bad military discharges, etc., is shared as appropriate. (The reader should know, however, that this sort of work is already underway under the auspices of the Defense Manpower Data Center. Additional funding may not be required.)

II-4. Analyze requirements for clearances, levels of classification, etc., and determine if numbers and levels can be reduced.

II-5. Work with DMDC to procure and integrate data bases covering, for instance: foreign travel, credit, IRS, Federal loans,

stocks, bonds, dividends, tax liens, prestigious mailing lists, law enforcement, health, etc. (This can be viewed as an expansion of I-8.)

II-6. Develop new techniques to supplement the background investigation, such as psychological and behavioral tests.

II-7. Investigate feasibility of the subject providing additional information to establish bona fides.

II-8. Develop a Personal History Statement for use in DoD.

II-9. Develop a personnel security management information system.

II-10. Develop a cost-benefit framework for evaluating personnel security programs and proposals.

Priority III Research Projects[1]

III-1. Describe screening procedures used by the U.S., other Governments, and in industry.

III-2. Develop and try out a new biographical questionnaire and subject interview procedure for use at Military Entrance Processing Stations (MEPS).

III-3. Develop pre-employment questionnaires for industrial security application.

III-4. Develop a prescreening process for use with special access program candidates.

III-5. Evaluate and validate information obtained in background investigations for enlistees discharged for unsuitability.

III-6. Conduct exit interviews of military personnel discharged for unsuitability to identify factors associated with their failure.

III-7. Develop and try out new interview-oriented background investigation procedures for initial and bring-up investigations.

III-8. Investigate the practicality of obtaining, and the usefulness of, Internal Revenue Service (IRS) data.

III-9. Investigate how to clear foreign-born personnel, e.g., engineers and scientists.

III-10. Analyze workload, skill, training and other features of Personnel Investigation Center (PIC) controllers' jobs.

---

[1]Our copy of the research agendas shifts to the use of the word *projects* in describing the last 33 tasks, instead of *efforts*. We have assumed that there is no significance in that change—that the words could have been used interchangeably in their meaning here—but we have retained the wording used in the original.

III-11. Develop, with Defense Investigative Service (DIS), measures of quality-of-investigation, ways to ensure high-quality investigations, and mechanisms for rewarding investigators.

III-12. Work with DIS and others to increase the scope of law enforcement records available to DIS and to improve the speed of access to those records.

III-13. Determine how veridical individuals are when they are interviewed by DIS investigators, and how to improve upon the openness and honesty of those interviewed. (Probably not needed if I-3 is successfully executed.)

III-14. Analyze how psychiatrists and psychologists arrive at their adjudicative recommendations.

III-15. Determine if an expert-systems approach can improve adjudication.

III-16. Evaluate: (1) the Services' Personnel Reliability Program (PRP), and (2) feasibility of using the PRP as a model for continuing evaluation in other sensitive positions.

III-17. Determine relationships between background investigation information and personnel, medical, and investigative records for enlistees discharged for unsuitability from high-risk jobs.

III-18. Follow up personnel in high-risk jobs whose background investigations become "issue" cases—how they are performing?

III-19. Develop post-clearance security risk indicators. (This can be viewed as an expansion of I-9.)

III-20. Defense Intelligence Agency (DIA) pre-employment interviews yield derogatory information from already cleared individuals—what can we learn about the clearance process from this?

III-21. Review economics-of-crime literature and determine implications for continuing evaluation of cleared individuals. (This item is related to I-9.)

III-22. Analyze disincentives for reporting security violations.

III-23. Determine relationship (if any) of foreign travel to espionage.

III-24. Evaluate the Vance program, and other programs, to determine if they minimize potential for compromise from personnel with sensitive information.

III-25. Determine comparative validity of various physiological assessment measures in identifying concealed offense history.

III-26. Develop procedural controls which would reduce the investment in security clearances.

III-27. Identify high risk/high leverage billets; develop a way of assessing security importance of billets.

III-28. Identify means to develop in organizations a pro-security ethic compatible with traditional American values.

III-29. Review statistical literature to identify techniques that might be used in predicting personnel security risks.

III-30. Investigate automated reporting of adverse information regarding cleared personnel.

III-31. Revalidate GAO's study on costs of delayed clearances.

III-32. What can we learn about granting of clearances from experiences of parole boards?

III-33. Compare select-in versus select-out security clearance granting perspectives and their implications for the security clearance process.

176 RESEARCH (TAB) QUESTIONS

Tab 1[2]

Compare/contrast results of Interview-oriented Background Investigation (IBI) and Special Background Investigation (SBI).[3]

Questions to be answered in this research:

1. Is 15 year SBI more productive than IBI? If yes, why?
2. Which produces more adverse or favorable information relevant to adjudication?
3. Which is more efficient/resource intensive? — Investigator's time, subject's time, employer's time, etc.
4. Could IBI replace SBI, i.e., could we go to single scope?
5. How important is flexibility by agents in conducting background investigations?
6. Which requires higher investigator skills?
7. If SBI is better, can IBI be improved to equal SBI?
8. Is there a product superior to either the IBI or SBI?
9. Who controls investigations, i.e., who decides on scope and coverage?

[2]Tab 1 refers to the set of questions that expand upon or amplify Task 1 of the Priority I Research Efforts. Tab 2 then expands upon Task 2, and so on, for the first nine tasks of the Priority I Research Efforts.

[3]In the original, it was noted that Tabs 1 and 3 are closely related.

10. What causes differences between SBI vs. IBI?
11. What should be in report to adjudicators?
12. What are agents' preferences, and why, and does this influence agent productivity?
13. What are adjudicators' preferences *re* IBI and SBI, and why?
14. Why does intelligence community prefer SBI?
15. What should coverage period be for either product?
16. How do interviewees, e.g., subjects, view interviews?
17. Which (IBI or SBI) yields fewer problem individuals upon longitudinal follow-up?
18. Does subject see interview as threat or deterrent, and even deter person from applying for job?
19. Which yields more openness and greater truthfulness?
20. What steps does agent take after interview, e.g., stop investigation, broaden investigation?
21. Would a branching approach to interviewing be more effective?
22. Are there tradeoffs among interview/non-interview, coverage and scope/years of coverage?

Tab 2

Validate existing criteria for personnel security clearance determinations, and develop more objective, uniform and valid adjudication standards, e.g., develop nexus with respect to the various criteria.[4]

Questions to be addressed in this research·

1. Do different adjudicators assume different relationships between information about people and their trustworthiness?
2. Is there evidence showing relationships between adjudicative criteria and performance for particular jobs at particular levels of clearance?
3. Could an actuarial approach be used? (Need outcomes, like car accidents for car insurance actuarial tables.)
4. Are lonely employees more vulnerable than other personnel to approaches by hostile agents?
5. What is impact of case law and administrative decisions on
   - Civil Service
   - Industrial clearances

[4]In the original, it was noted that Tabs 2, 6, and 7 are closely related.

6. Does desire to succeed lead to security violations?
7. Compare our hiring philosophy with that in private sector.
8. How do private organizations, e.g., Brinks, Wall Street brokers, make decisions?
9. Is "manipulability by others" measurable and predictive?
10. What should criteria for adjudication be?
11. Did caught-spies have derogatory information available to adjudicators at the time of adjudication?
12. How do you measure the adjudicative criteria?
13. We need a typology of security outcomes—spying, security violation, industrial espionage, theft, carelessness, PRP.
14. What do courts, Congress, public and interest groups expect *re* nexus?
15. What are formal vs. informal reasons for clearance revocation? Are formal and informal criteria different?
16. Should there be some reasons for turndowns or revocations for which there's no rebuttal or appeal?
17. Have changes in our culture required us to change our clearance criteria?
18. Can we rationalize the disposition of the cases of individuals who have committed adultery and the disposition of the cases of homosexuals in the adjudicative process? Likewise, the cases of individuals who abuse alcohol and the cases of those who abuse other drugs?
19. Is there a quota system on turning down people for clearances?
20. Which criteria have strongest/weakest links to turndown/approvals, and chances of holding up under review?
21. What role does and should due process play in nexus?
22. Given current criteria, what is probability of success in sustaining a denial?
23. Are we making moral judgments or security determinations during adjudication?
24. How do you define security risk?
25. Does literature on theft, computer crime, white-collar crime provide ideas for security clearance adjudication?
26. Should risk be expanded from selling secrets to theft-in-general, white-collar crime, etc.?

27. Do we treat blue-collar personnel differently from white-collar personnel, i.e., do we have different nexi for different levels of personnel?
28. Can we develop a profile indicative of susceptibility to approach by hostile agents?
29. Are child abuse victims security risks?
30. Can psychological tests be used to predict risks?

Tab 3

Investigate the design of the investigative interview—sequencing of questions, psychological context, etc., and determine how to ensure the openness and honesty of those interviewed.[5]

Questions to be answered in this research:

1. How do we get the most truthful interview?
2. What should be included in the interview?
3. In basic reference interview, how much time is needed to establish credibility and get interviewee to be reactive?
4. How do you train agents to be interviewers?
5. How do you prevent "rotedrill" and keep peak performance by interviewers? – Would a branching tree approach to interviewing be helpful?
6. How do you structure the interview: introduction, rapport, verification, investigation/reactive/probing phase, closure?
7. How do you establish psychological context for the interview?
8. Is interviewer variability a problem?
9. What are interviewers doing well, not well?
10. What do expert interviewers do that is different from other interviewers?
11. What are the roles of body language, nonverbals, clothes, gender, race, age, etc. of interviewers?
12. What is *the* purpose of the investigative interview?
13. How do you establish rapport and credibility with the interviewee?
14. What is the role of life-style questions?
15. How do you train interviewer to realize he already has answer—rather than "going rote"?

[5]In the original, it was noted that Tabs 1 and 3 are closely related.

Tab 4

Analyze efficacy of current continuing evaluation programs, e.g., is the periodic reinvestigation a good deterrent?

Questions and objectives to be addressed in this research:

A. Continuing Evaluation Programs:
   1. What kind of continuing evaluation programs exist within DoD? Describe.
   2. Evaluate effectiveness of DoD's continuing evaluation programs.
   3. Examine and describe other agencies' (non-DoD) continuing evaluation programs, to include assessment of their effectiveness.
   4. What are adverse action rates within DoD, and what are sources of derogatory data resulting in adverse action?
   5. Is *counseling* a part of the continuing evaluation program?
   6. What is the role of the individual, co-worker and supervisor in the continuing evaluation program?
   7. Describe and evaluate effectiveness of continuing evaluation programs.
   8. What is the interrelationship between security posture at front end, i.e, initial hiring, and continuing evaluation programs?
   9. How do adjudicators weight *historical* derogatory and *current* performance data?
   10. Describe and evaluate contractor's continuing evaluation programs.
   11. Compare contractor reporting with that of DoD's civilian/military programs.
   12. Should urinalysis be included in continuing evaluation program?
   13. Assess use of polygraph in continuing evaluation program.
   14. Examine DIA's interview program for cleared personnel joining the agency.
   15. What is the nature of the continuing evaluation procedures in the White House support activity program?

B. Periodic Reinvestigations (PR)
   1. What are the *objectives* and *expectations* of the PR?

2. What is the deterrent value of the PR?
3. What is the cost-effectiveness of the PR program?
4. Identify the segments of PR most productive of significant information.
5. What is the most appropriate scope for PR?
6. Should the PR include a psychological assessment component?
7. What other techniques may be effective for the PR?
8. What are the civil liberties considerations in PR?
9. Do PR's require unique investigative skills, abilities and experience?
10. Should PR's be conducted by an independent group *outside* DIS?
11. Analyze the effectiveness of subordinate, peer and supervisory interviews in PRs.

Tab 5

Analyze causes and factors in security violations by cleared personnel and develop security violations data base.

Questions to be addressed in this research:

1. How big is the security violation problem?
2. What is the distribution of incidents by agency, department, contractor, type of incident, etc.?
3. What has been the trend in numbers and types of violations?
4. Can we describe and evaluate current violation reporting systems?
5. What is DoD's policy on reporting violations?
6. What are the disincentives and incentives for reporting violations?
7. What would managers do in terms of disciplinary steps if they had a perfect or ideal reporting system available to them?
8. What characteristics differentiate organizations having high and low reported violation frequencies?
9. What systems are in force to monitor security violations?
10. What is the role of communication security telephone monitoring?
11. What is the correlation of frequency of incidence of security violations with reliability, untrustworthiness, loyalty?

12. What are the punitive measures, if any, in effect to deter violators—should they be changed, improved?
13. Who investigates violations—what are qualifications—disincentives?
14. Do centralized security violation data bases exist in the DoD components?
15. Is a centralized violation data base feasible and desirable?
16. Do model programs exist for reporting, acting on security violations?
17. Is there preferential treatment for certain classes of violators?
18. What training-to-report mechanisms exist, and are they effective?
19. How many security violations are known to coworkers or supervisors but not reported? Are there patterns in these failures? If there is a problem, how do we remedy it?

Tab 6

Analyze factors causing differences in negative adjudication rates among agencies and types of applicants.[6]

Questions to be addressed in this research:

1. Are there differences between individual and/or agency adjudicative decisions, e.g., does same case get treated differently?
   - Inter-organizational differences
   - Intra-organizational differences
   - Intra-adjudicator variability over time, e.g., learning or fatigue
2. Why do we send clean cases to adjudicators?
3. Is there a fatigue factor that affects adjudicators?
4. Is there a burnout factor that affects adjudicators?
5. What are factors contributing to differences in adjudication rates?
   - Skills, aptitudes and training.
   - Grade structure, promotion opportunities, career structure.
   - Organizational practices, e.g., organizational expectations, organizational pressures to produce.
   - Are you there to screen-in or -out?

[6]In the original, it was noted that Tabs 2, 6, and 7 are closely related.

6. What are adjudication rates and workloads, by clearance level and nature of project (visibility, level of secrecy, e.g., Black Programs)?
7. What are effects of adjudicators' prejudices? (If they have prejudices . . .)
8. Is there feedback for adjudicators?
9. Are there consequences for adjudicators' decisions, e.g., pressures to go fast, be correct, etc.?
10. Are adjudicative guidelines *different among* adjudicators and agencies?
11. What happens when adjudicators get an inadequate or very old investigation—is there pressure to keep moving?
12. Are adjudicative facilities adequately staffed?
13. Do adjudication rates differ by criterion?
14. How clear-cut are adjudicative criteria?
15. How well defined, formally and informally, are adjudicative criteria?
16. Do adjudicators have all the information they need?
17. What are effects of adjudicators' perceptions of right and wrong—Do adjudicators worry about effects on candidates turned down for clearances?
18. Are adjudicators' data and decisions amenable to an expert systems approach?
19. Are there gender, age and race effects in adjudicators' decisions?
20. What are personnel turnover and morale data like for adjudicators?
21. Is it practicable and desirable to centralize adjudication in DoD? At what levels?
22. Describe and compare the several adjudication programs in DoD and elsewhere?
23. Estimate the consistency (reliability) of adjudicative decisions.

Tab 7

Identify relevant qualifications, characteristics, and capabilities of adjudicators, and develop selection and training guidelines for adjudicators.[7]

Questions to be addressed in this research:

1. How can adjudicators take information given them and yield a particular specific clearance recommendation?
2. Can adjudicators be specialists (credit, psychology, drug abuse specialists) vs. generalists?
3. How do you select adjudicators? Would psychological tests be useful?
4. How do adjudicators stay motivated? Is the job boring?
5. What would effects of screening-out vs. screening-in for clearances be on adjudicators?
6. Should there be required educational experience thresholds for adjudicators?
7. Should there be standard training for adjudicators?
8. What do adjudicators do, and what skills are required, e.g., writing skills?
9. What is impact of workload and backlog on adjudicators?
10. What office environment is best for the work of adjudication?
11. Which Office of Personnel Management (OPM) job class is appropriate; is a change needed?
12. Is advanced/continuing training needed?
13. What is impact of how job is defined, e.g., part of adjudication team vs. being an individual adjudicator, on qualifications required?
14. What are effects of investigators' summaries on adjudicators attitudes and adjudicators' skills required?
15. Would a mentoring system help adjudicators?
16. What do adjudicators' supervisors do?
17. Should clearance turndowns be reviewed by attorneys?
18. What are current qualifications of adjudicators?
19. Would qualifications of adjudicators be helped if they went out with investigators, went to investigation school, etc.?

[7] In the original, it was noted that Tabs 2, 6, and 7 are closely related.

20. What measures are used to appraise the quality of an adjudicator's job performance? Are these valid? Do they include feedback from the adjudicatee's post-adjudication security performance?
21. What dimensions, e.g., tolerance for ambiguity, differentiate excellent from poor adjudicators?
22. What are effects on adjudication of adjudicators' prejudices?
23. Do different agencies, clearance levels, etc., require different adjudicator qualifications?
24. Are there jobs similar to adjudicators' jobs in other organizations, e.g., bank loan officials, Wall Street arbitragers—comparably skilled, paid, etc.?
25. How do Command pressures, e.g., "Get the work out!", influence the jobs of adjudicators and their performance?
26. Would adjudication be improved if DoD established an accreditation board for adjudicators?
27. If summaries are available, do adjudicators use them rather than the raw data? If "yes," is anything lost?

Tab 8

Bring automated data bases, e.g., DMDC's, financial, travel, health, etc., to bear on investigations.[8]

Questions to be answered in this research:

1. What sorts of data would be useful; which types are available on automated data bases?
2. Would access to such data bases be useful during initial investigation and adjudication, periodic reinvestigations, and/or continuing evaluation?
3. What relevant data bases are currently in use by DMDC and other parts of the government?
4. Who would be the customers for the analyses done with data bases? What outputs would be useful to those customers?
5. What are the constraints on obtaining and using data bases, e.g., Privacy Act?
6. If we had useful data bases, would we initially use them only with high-risk individuals and/or high-risk jobs?

[8]In the original, it was noted that Tabs 8 and 9 are closely related.

Tab 9

Run records of cleared people against financial data bases to determine whether or not security-relevant financial problems exist — begin with individuals in sensitive positions.[9]

Questions to be answered in this research:

1. Can analytic methods be developed to identify high risk personnel having financial problems?
2. Can we identify those with financial problems as well as those with unexplained affluence?
3. Can we identify sudden changes in economic status?
4. What data bases would be useful? What is available and under what constraints, e.g., Privacy Act and Financial Privacy Act?
5. How does IRS target people for auditing?
6. Can financial disclosure be made a condition of work in high-risk jobs, and can such disclosure data be used with data from financial data bases to identify security risks?
7. Who would be the customers for analyses using such data bases? What would be useful to them?
8. What would be the due process issues associated with using such data bases?

[9]In the original, it was noted that Tabs 8 and 9 are closely related.

Appendix B

GLOSSARY OF TERMS RELATED TO PERSONNEL SECURITY

Access. The ability and opportunity to obtain knowledge of classified information. An individual, in fact, may have access to classified information by being in a place where such information is kept, if the security measures that are in force do not prevent him from gaining knowledge of such information.[1]

Adjudication. The process of evaluating investigative material to assess a person's loyalty, reliability, and trustworthiness to determine that entrusting the person with classified material (or assigning the person to sensitive duties) is clearly consistent with the interests of national security.[2]

Agent. In intelligence usage, one who is authorized or instructed to obtain or to assist in obtaining information for intelligence or counterintelligence purposes.[3]

Background Investigation. A personnel security investigation consisting of both record reviews and interviews with sources of information as prescribed in *DoD PSP*, App. B, par. 3, covering the most recent five years of an individual's life or since the 18th birthday, whichever is shorter, provided that at least the last two years are covered and that no investigation will be conducted [for the years] prior to an individual's 16th birthday.[4]

Case Officer. In CIA usage, the person in charge of agents who collect intelligence and perform other clandestine duties.[5]

Cipher. Any cryptographic system in which arbitrary symbols or groups of symbols represent units of plain text of regular length,

---

[1]*Personnel Security Program*, Department of Defense, Office of the Deputy Under Secretary of Defense (Policy), DOD 5200.2-R, January 1987, hereafter cited as *DoD PSP*, p. I-2.

[2]Developed from *DoD PSP*, p. VI-1; established definition not located.

[3]*Dictionary of Military and Associated Terms*, Department of Defense, The Joint Chiefs of Staff, JCS Pub. 1, June 1, 1979, hereafter cited as *JCS Pub. 1*.

[4]*DoD PSP*, p. I-2.

[5]Henry S. A. Becket, *The Dictionary of Espionage*, Dell Publishing Co., New York, 1986, hereafter cited as *Becket*.

usually single letters, or in which units of plain text are rearranged, or both, in accordance with certain predetermined rules.[6]

Classified Information. Official information or material that requires protection in the interests of national security and that is classified for such purposes by appropriate classifying authority in accordance with the provisions of Executive Order 12356.[7] Official information which has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated.[8]

Classified Matter. Official information or matter in any form or of any nature which requires protection in the interests of national security. See also *Unclassified Matter*.[9]

Code. Any system of communication in which arbitrary groups of symbols represent units of plain text of varying length. Codes may be used for brevity or security.[10]

Communications Intelligence. Technical and intelligence information derived from foreign communications by other than the intended recipient.[11]

Communications Security. The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes (a) cryptosecurity, (b) transmission security, (c) emission security, and (d) physical security of communication security materials and information.[12]

Compromise. The known or suspected exposure of clandestine personnel, installations, or other assets, or of classified information or material, to an unauthorized person.[13]

Confidential. National security information or material which requires protection and the unauthorized disclosure of which could reasonably be expected to cause damage to the national security.[14]

---

[6]*JCS Pub. 1.*

[7]*DoD PSP*, p. I-2.

[8]*JCS Pub. 1.*

[9]Ibid.

[10]Ibid.

[11]Ibid.

[12]Ibid.

[13]Ibid.

[14]Ibid.

Counterespionage. That aspect of counterintelligence designed to detect, destroy, neutralize, exploit or prevent espionage activities through identification, penetration, manipulation, deception and repression of individuals, groups or organizations conducting or suspected of conducting espionage activities.[15]

Counterintelligence. That aspect of intelligence activity which is devoted to destroying the effectiveness of inimical foreign intelligence activities and to the protection of information against espionage, individuals against subversion, and installations or material against sabotage.[16]

Critical-Sensitive Position. A civilian position within the Department of Defense meeting the following criteria (a) access to Top Secret information; (b) development or approval of plans, policies, or programs that affect the overall operations of the Department of Defense or a DoD Component; (c) development or approval of war plans, plans or particulars of future major operations or special operations of war, or critical and extremely important items of war, . . . (f) duties falling under Special Access Programs (or others).[17]

Cultivation. The process of establishing rapport with a possible source of information or a potential defector.[18]

Develop. To cultivate a sympathizer into becoming an active espionage agent, generally on ideological grounds.[19]

Emission Security. The component of communications security which results from all measures taken to deny unauthorized persons from deriving information of value from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems.[20]

Espionage. Actions directed toward the acquisition of information through clandestine operations.[21]

False Flag. Recruiting an agent or an informer through the guise of telling him the actual work will be done for another country or interest.[22]

Formerly Restricted Data. Information removed from the Restricted Data category upon a joint determination by the

---

[15]Ibid.

[16]Ibid.

[17]Developed from *DoD PSP*, p. III-1.

[18]*Becket.*

[19]Ibid.

[20]*JCS Pub. 1.*

[21]Ibid.

[22]*Becket.*

Department of Energy (or antecedent agencies) and the Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be adequately safeguarded as classified defense information.[23]

GRU. *Glavnoe Razvedyvatelnoe Upravlenie*, the chief intelligence directorate of the Soviet General Staff.[24]

Illegals. Trained intelligence officers sent abroad, often with false identities, who maintain no overt contact with their government.[25]

Industrial Security. That portion of national security concerned with the protection of classified information in the possession of industrial contractors to the Department of Defense or other user agencies.[26]

Informant. Person who wittingly or unwittingly gives information of intelligence value to an agent or the service for which he works.[27]

Information Security. The systems for creating and controlling classified information.[28]

Intelligence. The product resulting from the collection, processing, integration, analysis, evaluation and interpretation of available information concerning foreign countries or areas.[29]

KGB. *Komitet Gosudarstvennoe Bezopastnosti*, the committee for state security of the Soviet Union.[30]

Limited Background Investigation. An investigation consisting of a subject interview (if the subject is a federal employee only), personal interviews with selected sources covering specific areas of the subject's background during the most recent one to three years, and written inquiries and record searches for a total of five years.[31]

---

[23]*JCS Pub. 1.*

[24]*Becket.*

[25]*Meeting the Espionage Challenge: A Review of United States Counterintelligence and Security Programs*, Report of the Select Committee on Intelligence, United States Senate, 99th Congress, 2nd Session, Report 99-522, hereafter cited as *Review*, p. 21.

[26]*Review*, p. 156.

[27]*Becket.*

[28]Developed; established definition not located.

[29]*JCS Pub. 1.*

[30]*Becket.*

[31]Developed from *Federal Government Security Clearance Program*, Hearings Before the Permanent Subcommittee on Investigation of the Committee on Governmental Affairs, United States Senate, 99th Cong., 1st Sess., S. Hrg. 99-166, hereafter cited as *Hearings*, p. 817.

MICE. Acronym for money, ideology, compromise, ego; the most common motivations impelling a foreigner to espionage.[32]

Minimum Background Investigation. An investigation consisting of the National Agency Check and Inquiries and a credit search. Telephone inquiries are made whenever the initial coverage of written inquiries is not returned, to insure that adequate coverage is obtained.[33]

National Agency Check. A personnel security investigation consisting of a records review of certain national agencies such as prescribed in *DoD PSP*, App. B, par. 1, including a technical fingerprint search of the files of the Federal Bureau of Investigation (FBI).[34]

National Agency Check plus Written Inquiries. A personnel security investigation conducted by the Office of Personnel Management, combining a National Agency Check and written inquiries to law enforcement agencies, former employees and supervisors, references and schools.[35]

National Security. A collective term encompassing both national defense and foreign relations of the United States.[36]

National Security Information. Information which requires protection in the interest of national defense or foreign relations of the United States and classified in accordance with Executive Orders which does not fall within the definition of Restricted Data or Formerly Restricted Data.[37]

Need-to-know. A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge, or possession of the classified information in order to perform tasks or services essential to the fulfillment of an official United States Government program. Knowledge, possession of, or access to, classified information shall not be afforded to any individual solely by virtue of the individual's office, position, or security clearance.[38]

---

[32]John Barron, *KGB Today. The Hidden Hand*, Reader's Digest Press, New York, 1983, p. 99.

[33]Developed from *Hearings*, p. 816.

[34]*DoD PSP*, p. I-4.

[35]*DoD PSP*, p. I-4.

[36]*JCS Pub. 1*.

[37]*Hearings*, p. 788.

[38]*DoD PSP*, p. I-4.

Noncritical-Sensitive Position. A civilian position within the Department of Defense meeting the following criterion: (a) access to Secret or Confidential information (or others).[39]

Nonsensitive Position. All civilian positions in the Department of Defense not designated as Critical-Sensitive (i.e., requiring access to Top Secret information) or Noncritical-Sensitive (i.e., requiring access to Secret or Confidential information).[40]

Official Information. Information which is owned by, produced by, or is subject to the control of the United States Government.[41]

Operations Security. The protection of military operations and activities resulting from the identification and subsequent elimination or control of indicators susceptible to hostile exploitation.[42]

Periodic Reinvestigation. An investigation conducted every five years for the purpose of updating a previously completed background or special investigation on persons occupying positions referred to in *DoD PSP*, pars. 3-700 through 3-710.[43]

Personnel Security. A composite activity consisting of (1) the security discipline concerned with protecting classified information through measures appropriate for persons who (a) are seeking, (b) have, or (c) have had authorized access to classified information; and (2) selected aspects of personnel suitability for (a) acceptance and retention of personnel in the Armed Forces, and (b) the assignment of DoD personnel to sensitive positions not requiring access to classified information.[44]

Physical Security. That part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, facilities, material, and documents, and to safeguard them against espionage, sabotage, damage, and theft.[45]

Restricted Area. An area under military jurisdiction in which special security measures are employed to prevent unauthorized entry.[46]

Restricted Data. Data which is defined in Sec. IIy of the Atomic Energy Act of 1954, as amended, as ". . . all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the

---

[39]Developed from *DoD PSP*, p. III-2.

[40]Ibid.

[41]*JCS Pub. 1.*

[42]Ibid.

[43]*DoD PSP*, p. I-4.

[44]Developed from DoD usage; established definition not located.

[45]*JCS Pub. 1.*

[46]Ibid.

production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Sec. 142."[47]

Sabotage. An act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war material, premises or utilities to include human and natural resources.[48]

Scientific and Technical Intelligence. The product resulting from the collection, evaluation, analysis, and interpretation of foreign scientific and technical information which covers: (a) foreign developments in basic and applied research in applied engineering techniques; and (b) scientific and technical characteristics, capabilities and limitations of all foreign military systems, weapons, weapon systems, and materiel, the research and development related thereto, and the production methods employed for their manufacture.[49]

Secret. National security information or material which requires a substantial degree of protection and the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security.[50]

Security. A condition which prevents unauthorized persons from having access to official information which is safeguarded in the interests of national security.[51]

Sensitive Compartmented Information. All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established.[52]

Sensitive Position. Any position so designated within the Department of Defense, the occupant of which could bring about, by virtue of the nature of the position, a materially adverse effect on the national security.[53]

---

[47]*Hearings*, p. 788.

[48]*JCS Pub. 1.*

[49]Ibid.

[50]Ibid.

[51]Ibid.

[52]Ibid.

[53]*DoD PSP*, p. I-5.

Special Access Program. Any program imposing "need-to-know" or access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information.[54]

Special Background Investigation. A personnel security investigation consisting of all the components of a Background Investigation plus certain additional investigative requirements as prescribed in *DoD PSP*, App. B, par. 4.[55]

Spy. According to the Hague Convention of 1899, "One who, acting clandestinely or on false pretenses, obtains, or seeks to obtain, information in the zone of operations of a belligerent with the intention of communicating it to a hostile party." This definition would eliminate intelligence analysts, code and cipher clerks, and others in intelligence who are not operatives.[56] More generally, one employed by a government to obtain secret information or intelligence about another country, especially with reference to military or naval affairs.[57]

Subversion. Action designed to undermine the military, economic, psychological, morale or political strength of a regime.[58]

Technical Information. Information, including scientific information, which relates to research, development, engineering, test, evaluation, production, operation, use and maintenance of munitions and other military supplies and equipment.[59]

Technical Intelligence. See *Scientific and Technical Intelligence.*

Technical Surveillance Countermeasures. Measures for the impairment of the effectiveness of hostile surveillance by national technical means.[60]

Top Secret. National security information or material which requires the highest degree of protection and the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security.[61]

Unclassified Matter. Official matter which does not require the application of security safeguards, but the disclosure of which may

---

[54]Ibid.

[55]Ibid.

[56]Bob Burton, *Top Secret: A Clandestine Operator's Glossary of Terms*, Berkley Publishing Corp., New York, 1987.

[57]Developed; modern definition not located.

[58]*JCS Pub. 1.*

[59]Ibid.

[60]Developed; established definition not located.

[61]*JCS Pub. 1.*

be subject to control for other reasons. See also *Classified Matter*.[62]

Witting. A person who knowingly cooperates with an intelligence agency.[63]

---

[62]Ibid.

[63]*Becket*.

Appendix C

ANALYSIS OF THE CURRENT RESEARCH AGENDAS, BY SUBJECT

INTRODUCTION

The analysis in Sec. III of this report views the current research agendas as a whole, looking for structure, emphasis, patterns, and anomalies. This appendix provides a narrower-scope examination of the agendas *within* the context of the subjects they address. The questions explored here are more limited: Given that the current research agendas address this particular subject, are there any obvious gaps, and if so, what should fill them?

The subjects are taken up in the order of their frequency of appearance in the current research agendas. Only the 53 tasks are considered, and the relative importance or priority of subjects is not argued. Within any subject, the tasks are grouped by the aspect of the subject addressed (e.g., evaluation, improvement, cost, etc.) and then listed in order of their appearance in the agendas (see App. A).

INVESTIGATION

Eighteen of the 53 tasks in the current research agendas appear to to deal with the subject of investigation;[1] they are about evenly divided among three aspects:

1. Additional sources of information for investigations.
2. Evaluation of current investigative procedures.
3. Design and development of improved investigative procedures.

Six of the 18 tasks associated with investigation explore additional sources of information for investigations:

1. Bring automated data bases, e.g., Defense Manpower Data Center's (DMDC), financial, travel, health, etc , to bear on investigations. [I-8]

[1]See Table 1 of Sec. III for the breakdown of the 53 tasks by subject.

2. Develop automated data systems insuring that information about people who lost clearances, had bad military discharges, etc., is shared as appropriate. (The reader should know, however, that this sort of work is already underway under the auspices of the Defense Manpower Data Center. Additional funding may not be required.) [II-3]
3. Work with DMDC to procure and integrate data bases covering, for instance: foreign travel, credit, IRS, Federal loans, stocks, bonds, dividends, tax liens, prestigious mailing lists, law enforcement, health, etc. (This can be viewed as an expansion of I-8.) [II-5]
4. Investigate feasibility of the subject providing additional information to establish bona fides. [II-7]
5. Investigate the practicality of obtaining, and the usefulness of, Internal Revenue Service (IRS) data. [III-8]
6. Work with DIS and others to increase the scope of law enforcement records available to DIS and to improve the speed of access to those records. [III-12]

Five of the 18 tasks associated with investigation address the evaluation of current investigative procedures:

1. Compare/contrast results of interview-oriented background investigation (IBI) and the special background investigation (SBI). [I-1]
2. Analyze productivity and effectiveness of current personnel security information collection procedures and information sources, e.g., neighborhoods, schools, peers, roommates; written inquiries to employers. [I-10]
3. Evaluate and validate information obtained in background investigations for enlistees discharged for unsuitability. [III-5]
4. Determine relationships between background investigation information and personnel, medical, and investigative records for enlistees discharged for unsuitability from high-risk jobs. [III-17]
5. Determine comparative validity of various physiological assessment measures in identifying concealed offense history. [III-25]

Five of the 18 tasks associated with investigations address the design and development of improved procedures for investigations:

1. Investigate the design of the investigative interview—sequencing of questions, etc.—determine how open and honest

individuals are when they are interviewed by DIS investigators, and how to improve upon openness and honesty of those interviewed. [I-3]
2. Develop new techniques to supplement the background investigation, such as psychological and behavioral tests. [II-6]
3. Develop a Personal History Statement for use in DoD. [II-8]
4. Develop and try out new interview-oriented background investigation procedures for initial and bring-up investigations. [III-7]
5. Analyze workload, skill, training and other features of Personnel Investigation Center (PIC) controllers' jobs.[2] [III-10]

Finally, two of the 18 tasks associated with investigation address both the evaluation and improvement of current procedures:

1. Develop, with Defense Investigative Service (DIS), measures of quality-of-investigation, ways to ensure high-quality investigations, and mechanisms for rewarding investigators. [III-11]
2. Determine how veridical individuals are when they are interviewed by DIS investigators, and how to improve upon the openness and honesty of those interviewed. (Probably not needed if I-3 is successfully executed.) [III-13]

Thus, the current research agendas would explore ways to evaluate and improve investigations with respect to their data or procedures. Whether the agendas include all the possibilities for new data or the improvement of procedures is moot, but the evaluation of investigation as a principal (implied) focus of the personnel security program is obviously missing some key aspects, including the following:

1. *Costs:* What are the direct and indirect[3] costs of investigation? How do the costs vary with the utility or pertinence of the information acquired?[4]

---

[2]The Personnel Investigation Center, in Baltimore, controls all personnel security investigations for the DoD, except special clearance programs. At the request of DISCO, PIC initiates and controls the investigations, identifies the investigative leads from the personal history (Form 398), manages the National Agency Check, sends directives to the field offices to pursue leads, and then assembles the responses into a final investigation report.

[3]The indirect costs would presumably include the societal costs of employment delays, the time spent by subjects and respondents in supplying information, etc.

[4]For example, does some information, such as that obtained from a National Agency Check, typically have a higher utility-to-cost ratio than interviews with neighbors? The question is really about the "return on investment" curve for investigations as they seek more and more information.

2. *Tradeoffs:* How do investments in investigation trade off with related activities in the personnel security program? Would it be more effective to put additional efforts (on the margin) into investigation than into adjudication?
3. *Alternatives:* Are there completely different alternative approaches that could be substituted for investigation? Could the personnel security program be built upon completely different foundations, such as those used for employment outside the U.S. government or its contractors?[5]

The current research agendas do not significantly challenge or measure the role of investigations. Indeed, investigation appears to be accepted as something to be improved to the extent feasible rather than tested for its worth or necessity.

MONITORING

Eleven of the 53 tasks in the current research agendas appear to address monitoring the behavior of currently cleared personnel. The tasks are about evenly split between the evaluation of current procedures and the design or development of improved procedures for the monitoring of cleared personnel. Six of the 11 tasks deal with the evaluation of current procedures:

1. Analyze efficacy of current continuing evaluation programs, e.g., is the periodic investigation a good deterrent? [I-4]
2. Evaluate: (1) the Services' Personnel Reliability Program (PRP), and (2) feasibility of using the PRP as a model for continuing evaluation in other sensitive positions. [III-16]
3. Follow up personnel in high-risk jobs whose background investigations become "issue" cases—how they are performing? [III-18]
4. Analyze disincentives for reporting security violations. [III-22]
5. Determine relationship (if any) of foreign travel to espionage. [III-23]
6. Evaluate the Vance program, and other programs, to determine if they minimize potential for compromise from personnel with sensitive information. [III-24]

[5]This may be the thrust of questions 2-7 and 2-8; but if so, the issue has sufficient stature and poses a sufficient intellectual challenge to warrant a separate research task.

Five of the 11 tasks deal with the design and development of improved procedures for monitoring the behavior of currently cleared personnel:

1. Analyze causes and factors in security violations by cleared personnel, and develop security violations data bases. [I-5]
2. Run records of cleared personnel against financial data bases to determine whether problems exist—develop a system for use with people in sensitive positions. [I-9]
3. Develop post-clearance security risk indicators. (This can be viewed as an expansion of I-9.) [III-19]
4. Review economics-of-crime literature and determine implications for continuing evaluation of cleared individuals. (This item is related to I-9.) [III-21]
5. Investigate automated reporting of adverse information regarding cleared personnel. [III-30]

Thus, the current research agendas would explore ways to evaluate and improve investigations with respect to their data or procedures. Whether the agendas include all the possibilities for new data or the improvement of investigative procedures is moot, but the focus on the evaluation of the investigative process clearly neglects several other key issues, including the following:

1. *Costs:* What are the direct and indirect[6] costs of monitoring? How do the costs vary with the extent and utility of the monitoring efforts?
2. *Tradeoffs:* How do investments in monitoring trade off with related activities in the personnel security program? Would it be more effective to put additional efforts (on the margin) into initial screening or investigation of candidates than into monitoring?
3. *Approaches:* Are there completely different alternative approaches that could be substituted for monitoring? Could the personnel security program be built upon completely different foundations, such as supervisors *vouching* for the continuing trustworthiness of all immediate subordinates on the pain of their own dismissal?

[6]The indirect costs would presumably include the subjective societal costs of intrusions or invasions into matters that American society has traditionally treated as personal or private. Depending upon the means chosen for monitoring, there may also be "chilling" effects on working relationships, with consequences that will be difficult to project except through large-scale, long-term experiments.

4. *Roles:* Should the role of monitoring be limited to currently cleared personnel? Or should it be extended to personnel whose clearances have been revoked? Should monitoring have as its objective warning (of security failures) or continued well-being (of personnel)?[7]

The treatment of monitoring in the current research agendas has the flavor of a difficult responsibility that is being assumed belatedly and with reluctance. There is no evidence that it is seen as a potential opportunity for a major reorientation or improvement of the personnel security program. Indeed, the research tasks on monitoring suggest that it is a personnel security function undertaken more with distaste than with excitement.

CLEARANCES

Seven of the 53 tasks in the current research agendas address the subject of clearances. Six of these explore the design and development of new procedures for the granting, denying, and revoking of clearances:

1. Analyze requirements for clearances, levels of classification, etc., and determine if numbers and levels can be reduced. [II-4]
2. Investigate how to clear foreign-born personnel, e.g., engineers and scientists. [III-9]
3. Defense Intelligence Agency (DIA) pre-employment interviews yield derogatory information from already cleared individuals—what can we learn about the clearance process from this? [III-20]
4. Develop procedural controls which would reduce the investment in security clearances. [III-26]
5. What can we learn about granting of clearances from experiences of parole boards? [III-32]
6. Compare select-in versus select-out security clearance granting perspectives and their implications for the security clearance process. [III-33]

[7]As currently configured, monitoring (continuing or periodic) appears to be aimed at warning against impending or ongoing breaches in security. It might also (or instead) be configured to ensure the continued well-being and satisfaction of personnel who are, or have been, cleared, as a bulwark against disloyal actions.

One of the seven tasks deals with the indirect cost of clearance delays:

> Revalidate GAO's study on costs of delayed clearances. [III-31]

Thus, most of tasks associated with clearances would support the design or development of improved procedures for the granting, denying, and revoking of clearances. Clearances are apparently accepted as the programmatic centerpiece: All major activities—screening, adjudication, monitoring, and investigation—lead to decisions about clearances. The possibility of *alternatives* to, or the elimination of, clearances is not obvious; but neither is it, apparently, to be the subject of research.

If clearances are accepted as the centerpiece of the personnel security program, they are the ideal springboard for *tradeoffs* among the activities that lead to clearances: How should screening, adjudication, and monitoring efforts be balanced for maximum program effectiveness at any given level of investment? And how should investigation efforts then be balanced in their support of screening, adjudication, and monitoring? A relatively simple, parametric model of these components should provide very useful information about basic design tradeoffs for the personnel security program. Such a model might show, for example, that the present program is badly balanced for any credible range of assumed performance capabilities for screening, adjudicating, and monitoring activities. Or, if one assumes that the program has been reasonably balanced by experience and intuition, then the model could be used to imply the relative performance capabilities for screening, adjudication, and monitoring.

The indirect costs of *delayed* clearances are addressed in Task III-31, but the direct and indirect *costs* of clearances—their granting, denial, and revocation—need examination and understanding.

SCREENING

Six of the 53 tasks in the current research agendas address the subject of screening. Four of these deal with the design and development of improved screening procedures:

1. Describe screening procedures used by the U.S., other Governments, and in industry. [III-1]

2. Develop and try out a new biographical questionnaire and subject interview procedure for use at Military Entrance Processing Stations (MEPS). [III-2]
3. Develop pre-employment questionnaires for industrial security application. [III-3]
4. Develop a prescreening process for use with special access program candidates. [III-4]

Two of the six tasks deal with the evaluation of current procedures for screening:

1. Evaluate the Services' prescreening procedures, e.g., the Army's MEPS questionnaire and the Navy's preservice drug and offense history inventory. [II-1]
2. Conduct exit interviews of military personnel discharged for unsuitability to identify factors associated with their failure. [III-6]

The research tasks associated with screening are more detailed and specific than those associated with other subjects. Some, perhaps most, are not research tasks as much as they are developmental or operational tasks (e.g., Tasks III-2 and III-3).

The emphasis on screening for military enlisted personnel (Tasks II-1, III-2, and III-6) invites inquiry and, hence, research about its relevance to civilian and commissioned officer personnel.

Absent from these tasks is research about alternative roles for screening, its direct and indirect costs, how it trades off with other activities, and the alternative approaches to screening.

ADJUDICATION

Five of the 53 tasks in the current research agendas address the subject of adjudication. Three of these deal with the evaluation of current adjudication procedures:

1. Validate existing criteria for personnel security clearance determinations, and develop more objective, uniform, and valid adjudication standards, e.g., develop nexus with respect to the various criteria. [I-2]
2. Analyze factors causing differences in negative adjudication rates among agencies and types of applicants. [I-6]
3. Identify relevant qualifications, characteristics, and capabilities of adjudicators, and develop selection and training guidelines for adjudicators. [I-7]

Two of the five deal with the design and development of improved procedures for adjudication:

1. Analyze how psychiatrists and psychologists arrive at their adjudicative recommendations. [III-14]
2. Determine if an expert-systems approach can improve adjudication. [III-15]

Adjudication is the linchpin of the current personnel security program.[8] It is gratifying, therefore, to see that Task I-2 seeks the jugular of the theory that serves as the foundation of the program. The (implied) theory may be stated as follows:

> The potential for *future* untrustworthy security behavior by an individual can be reliably discerned from a thorough investigation of that individual's past and present behavior and associations.

Validating the criteria for personnel security clearance determinations (through the adjudication process) is tantamount to validating the theory. Thus, Task I-2 could be the most important research question of the current agendas. Unfortunately, if one believes that the theory is not valid on its face and therefore cannot be validated, then Task I-2 will not be successfully completed as posed. As a research task, it might have been better aimed directly at the theory itself rather than at the adjudication criteria:

> Assess the validity of the theory that the potential for future untrustworthy security behavior by an individual can be reliably discerned from a thorough investigation of that individual's past and present behavior and associations.

Assessing the validity of one theory, of course, invites assessment of others, such as:

> Most individuals have the potential for untrustworthy security behavior under certain circumstances or situations, which will vary in quality and degree between individuals.

The remainder of the tasks would attempt to improve the quality of the adjudication process. Only one, Task III-14, would shed any additional light on the theory upon which the adjudication process stands.

---

[8]Most of the investigative effort is fed through the adjudication process, which is the principal means for granting and denying clearances, which, in turn, is the centerpiece of the personnel security program. The screening of candidates for clearances and the monitoring of behavior for the revoking of clearances are sideshows by comparison with the main axis of the program: adjudication of information acquired through investigation.

PROGRAM AND PROBLEMS

The program and problems were the two least addressed subjects of the seven originally identified in the current research agendas. Only three tasks were devoted to each of these two subjects. Since they received significantly less attention than any of the other five subjects, they were analyzed earlier as anomalies in the overall analysis of the agendas.

REFERENCES

Barron, John, *Breaking the Ring*, Houghton Mifflin Co., Boston, 1987.

——, *KGB Today: The Hidden Hand*, Reader's Digest Press, New York, 1983.

——, *KGB: The Secret Work of Soviet Agents*, Reader's Digest Press, New York, 1974.

Becket, Henry S. A., *The Dictionary of Espionage*, Dell Publishing Co., New York, 1986.

Burton, Bob, *Top Secret: A Clandestine Operator's Glossary of Terms*, Berkeley Books, New York, 1987.

"Defense Personnel Security Research and Education Center (PERSEREC)," Department of Defense Directive No. 5210.79, February 19, 1986.

Dewey, John, *Logic, The Theory of Inquiry*, Henry Holt and Co., New York, 1938.

Dictionary of Military and Associated Terms, Department of Defense, Joint Chiefs of Staff, JCS Pub. 1, June 1, 1979.

Federal Government Security Clearance Programs: Hearings Before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, U.S. Senate, 99th Cong., 1st Sess., S. Hrg. 99–166.

Fisher, Gene H., *Cost Considerations in Systems Analysis*, American Elsevier, New York, 1971.

Hall, Arthur D., *A Methodology for Systems Engineering*, D. Van Nostrand Co., Inc., Princeton, New Jersey, 1962.

Jones, R. V., *The Wizard War: British Scientific Intelligence, 1939–1945*, Coward, McCann & Geoghegan, Inc., New York, 1978.

Keeping the Nation's Secrets: A Report to the Secretary of Defense by the Commission to Review DoD Security Policies and Practices, Office of the Secretary of Defense, November 19, 1985.

Knightly, Phillip, *The Second Oldest Profession*, W. W. Norton & Co., New York, 1986.

Laqueur, Walter, *A World of Secrets: The Uses and Limits of Intelligence*, Basic Books, Inc., New York, 1985.

Meeting the Espionage Challenge: A Review of United States Counterintelligence and Security Programs, Report of the Select Committee on Intelligence, U.S. Senate, 99th Cong., 2d Sess., Report 99–522.

Morse, Philip M. and George E. Kimball, *Methods of Operations Research*, The Technology Press of Massachusetts Institute of Technology and John Wiley & Sons, 1st Rev. Ed., New York, 1951.

Personnel Security Program, Department of Defense, Office of the Deputy Under Secretary of Defense (Policy), DOD 5200.2-R, January 1987.

Pincher, Chapman, *Traitors: The Anatomy of Treason*, St. Martin's Press, New York, 1987.

Recent Espionage Cases, U.S. Department of Defense, Defense Security Institute, January 1987.

Saaty, Thomas L., *The Analytic Hierarchy Process*, McGraw-Hill, New York, 1980.

"Security Requirements for Government Employment," The White House, Executive Order 10450, April 27, 1953.

Suvorov, Victor, *Inside Soviet Military Intelligence*, Macmillan Publishing Company, New York, 1984.